User Manual

GEM 2M

LTE 4G M2M Router

www.proroute.co.uk

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION **8**

1.1 CONTENTS LIST *9*

1.2 HARDWARE INSTALLATION *10*

1.2.1 WARNING *10*

1.2.2 SYSTEM REQUIREMENTS *10*

1.2.3 Hardware Configuration *11*

1.2.4 LED Indication *13*

CHAPTER 2 GETTING STARTED **14**

2.1 HARDWARE INSTALLATION *14*

2.1.1 Mount the Unit *14*

2.1.2 Insert the SIM Card *14*

2.1.3 Connecting Power *15*

2.1.4 Connecting DI/DO Devices *16*

2.1.5 Connecting Serial Devices *16*

2.1.6 Connecting to the Network or a Host *17*

2.2 EASY SETUP BY CONFIGURING WEB UI *18*

2.2.1 Wizard *18*

2.2.1.1 Configure with the Network Setup Wizard 19

2.2.1.2 Configure with the VPN Setup Wizard 21

2.2.2 Status *25*

2.2.2.1 Network Status 26

2.2.2.2 LAN Client List 27

2.2.2.3 Firewall Status 28

2.2.2.4 VPN Status 29

2.2.2.5 System Management Status 30

CHAPTER 3 MAKING CONFIGURATIONS **31**

3.1 BASIC NETWORK *32*

3.1.1 WAN Setup *33*

3.1.1.1 Physical Interface 33

3.1.1.2 Internet Setup 34

3.1.1.2.1 3G/4G WAN – 3G/4G 35

3.1.2 LAN & VLAN Setup *39*

3.1.2.1 Ethernet LAN 39

3.1.2.2 VLAN 40

3.1.2.2.1 VLAN Scenarios 41

3.1.2.2.2 Port-Based VLAN 45
3.1.2.2.3 Tag-Based VLAN 46
3.1.3 IPv6 Setup 47
3.1.3.1 6 to 4 48
3.1.3.2 6 in 4 49
3.1.4 NAT / Bridging 51
3.1.4.1 Configuration 51
3.1.4.2 Virtual Server & Virtual Computer 52
3.1.4.2.1 Virtual Server 52
3.1.4.2.2 Virtual Computer 53
3.1.4.3 Special AP & ALG 53
3.1.4.4 DMZ 54
3.1.5 Routing Setup 55
3.1.5.1 Static Routing 55
3.1.5.2 Dynamic Routing 56
3.1.5.2.1 RIP 57
3.1.5.2.2 OSPF 57
3.1.5.2.3 BGP 58
3.1.5.3 Routing Information 59
3.1.6 Client/Server/Proxy 59
3.1.6.1 Dynamic DNS 59
3.1.6.2 DHCP Server 60
3.1.6.2.1 DHCP Server List 60
3.1.6.2.2 DHCP Server Configuration 61
3.1.6.2.3 Fixed Mapping 62
3.2 ADVANCED NETWORK 63
3.2.1 Firewall 63
3.2.1.1 Configuration 64
3.2.1.2 Packet Filters 64
3.2.1.2.1 Configuration 64
3.2.1.2.2 Packet Filter List 65
3.2.1.2.3 Packet Filter Rule Configuration 65
3.2.1.3 URL Blocking 67
3.2.1.3.1 Configuration 67
3.2.1.3.2 URL Blocking Rule List 67
3.2.1.3.3 URL Blocking Rule Configuration 68
3.2.1.4 Web Content Filters 69
3.2.1.4.1 Configuration 69
3.2.1.4.2 Web Content Filter Rule List 69

3.2.1.4.3 Web Content Filter Configuration 70
3.2.1.5 MAC Control 70
3.2.1.5.1 Configuration 71
3.2.1.5.2 MAC Control Rule List 71
3.2.1.5.3 MAC Control Rule Configuration 72
3.2.1.6 Application Filters 72
3.2.1.6.1 Configuration 73
3.2.1.7 IPS 73
3.2.1.8 Options 74
3.2.2 QoS & BWM 75
3.2.2.1 Configuration 76
3.2.2.2 Rule-based QoS 77
3.2.2.2.1 Configuration 78
3.2.2.2.2 QoS Rule List 78
3.2.2.2.3 QoS Rule Configuration 79
3.2.3 VPN Setup 83
3.2.3.1 Configuration 83
3.2.3.2 IPSec 84
3.2.3.2.1 IPSec VPN Tunnel Scenarios 84
3.2.3.2.2 IPSec Configuration 85
3.2.3.2.3 Tunnel List & Status 86
3.2.3.2.4 Tunnel Configuration 86
3.2.3.2.5 Local & Remote Configuration 87
3.2.3.2.6 Authentication 88
3.2.3.2.7 IKE Phase 88
3.2.3.2.8 IKE Proposal Definition 89
3.2.3.2.9 IPSec Phase 90
3.2.3.2.10 IPSec Proposal Definition 90
3.2.3.2.11 Manual Proposal 91
3.2.3.3 PPTP 91
3.2.3.3.1 PPTP / L2TP VPN Tunnel Scenarios 92
3.2.3.3.2 PPTP Server Configuration 93
3.2.3.3.3 PPTP Server Status 93
3.2.3.3.4 User Account List 94
3.2.3.3.5 User Account Configuration 94
3.2.3.3.6 PPTP Client 94
3.2.3.3.7 PPTP Client List & Status 95
3.2.3.3.8 PPTP Client Configuration 95
3.2.3.4 L2TP 96

3.2.3.4.1 L2TP Server Configuration 97
3.2.3.4.2 L2TP Server Status 98
3.2.3.4.3 User Account List 98
3.2.3.4.4 User Account Configuration 98
3.2.3.4.5 L2TP Client 99
3.2.3.4.6 L2TP Client List & Status 99
3.2.3.4.7 L2TP Client Configuration 99
3.2.3.5 GRE 101
3.2.3.5.1 GRE VPN Tunnel Scenario 101
3.2.3.5.2 GRE Configuration 101
3.2.3.5.3 GRE Tunnel Definitions 102
3.2.3.5.4 GRE rule Configuration 102
3.2.4 Redundancy 103
3.2.4.1 VRRP 103
3.2.5 System Management 104
3.2.5.1 TR-069 104
3.2.5.2 SNMP 105
3.2.5.3 Telnet with CLI 107
3.2.5.4 UPnP 108
3.2.6 Certificate 108
3.2.6.1 My Certificates 109
3.2.6.1.1 Root CA 109
3.2.6.1.2 Local Certificate List 111
3.2.6.2 Trusted Certificates 112
3.2.6.2.1 Trusted CA Certificate List 113
3.2.6.2.2 Trusted Client Certificate List 114
3.2.6.3 Issue Certificates 116
3.2.7 Communication Bus 117
3.2.7.1 Port Configuration 117
3.2.7.2 Virtual COM 117
3.2.7.3 Modbus 126
3.3 APPLICATIONS 128
3.3.1 Mobile Applications 128
3.3.1.1 SMS 128
3.3.1.2 USSD 130
3.3.1.3 Network Scan 132
3.3.1.4 Remote Management 132
3.3.2 IO Management 135
3.3.2.1 Configuration 135

3.4 SYSTEM 136
3.4.1 System Related 137
3.4.1.1 Change Password 138
3.4.1.2 System Information 138
3.4.1.3 System Status 139
3.4.1.4 System Tools 140
3.4.2 Scheduling 142
3.4.3 Grouping 143
3.4.3.1 Grouping Configuration 144
3.4.3.2 Host Grouping 144
3.4.3.2.1 Host Group List 144
3.4.3.2.2 Host Group Configuration 145
3.4.3.3 File Extension Grouping 145
3.4.3.3.1 File Extension Group List 145
3.4.3.3.2 File Extension Group Configuration 145
3.4.3.4 L7 Application Grouping 146
3.4.3.4.1 L7 Application Group List 146
3.4.3.3.2 L7 Application Group Configuration 146
3.4.4 External Servers 147
3.4.4.1 External Server List 148
3.4.4.2 External Server Configuration 148
3.4.5 MMI 149
3.4.5.1 Web UI 149

APPENDIX A. LICENSING INFORMATION 150

Copyright

The contents of this publication may not be reproduced in any part or as a whole, stored, transcribed in an information retrieval system, translated into any language, or transmitted in any form or by any means, mechanical, magnetic, electronic, optical, photocopying, manual, or otherwise, without the prior written permission.

Trademarks

All products, company, brand names are trademarks or registered trademarks of their respective companies. They are used for identification purpose only. Specifications are subject to be changed without prior notice.

Chapter 1 Introduction

Congratulations on your purchase of this outstanding product: Proroute GEM-2M 4G Router. For M2M (Machine-to-Machine) applications, GEM2M Cellular Gateway is absolutely the right choice. With built-in world-class 4G LTE module, you just need to insert a SIM card from local mobile carrier to get to Internet. The redundant SIM design provides a more reliable WAN connection for critical applications. Using VPN tunneling technology, remote sites easily become a part of a company Intranet, and all data is transmitted in a secure (256-bit AES encryption) link. To meet a variety of M2M application requirements, Proroute GEM-2M Cellular Gateway products are based on modular design.

This GEM 2M series product is loaded with superb security features including VPN, firewall, NAT, port forwarding, DHCP server and many other powerful features for complex and demanding business and M2M (Machine-to-Machine) applications. The redundancy design in fallback 9-48 VDC power terminal, dual SIM cards and VRRP function makes the device as a back-up in power, network connection and data transmission without lost.

Main Features:

- Provide 3G/LTE WAN connection.
- Support dual SIMs for the redundant wireless WAN connection.
- Provide one Ethernet port for comprehensive LAN connection.
- Feature with VPN and NAT firewall to have powerful security.
- Support the robust remote or local management to monitor network.
- Designed by solid and easy-to-mount metal body for business and M2M environment to work with a variety M2M (Machine-to-Machine) applications.

Before you install and use this product, please read this manual in detail to fully explore the functions of this product.

1.1 Contents List

Items	Description	Contents	Quantity
1	**GEM-2M series 4G Router**		1pcs
2	**Cellular Antenna**		2pcs
3	**Power Adapter (DC 12V/2A)** (*[1])		1pcs
4	**DC Jack Converter**		1pcs
5	**RJ45 Cable**		1pcs
6	**Console Cable**		1pcs
7	**CD (Manual)**		1pcs
8	**Mounting Bracket**		2pcs
9	**DIN-Rail Bracket**		1pcs

1 The maximum power consumption of GEM-2M series is 15.6W.

1.2 Hardware Installation

1.2.1 WARNING

Attention

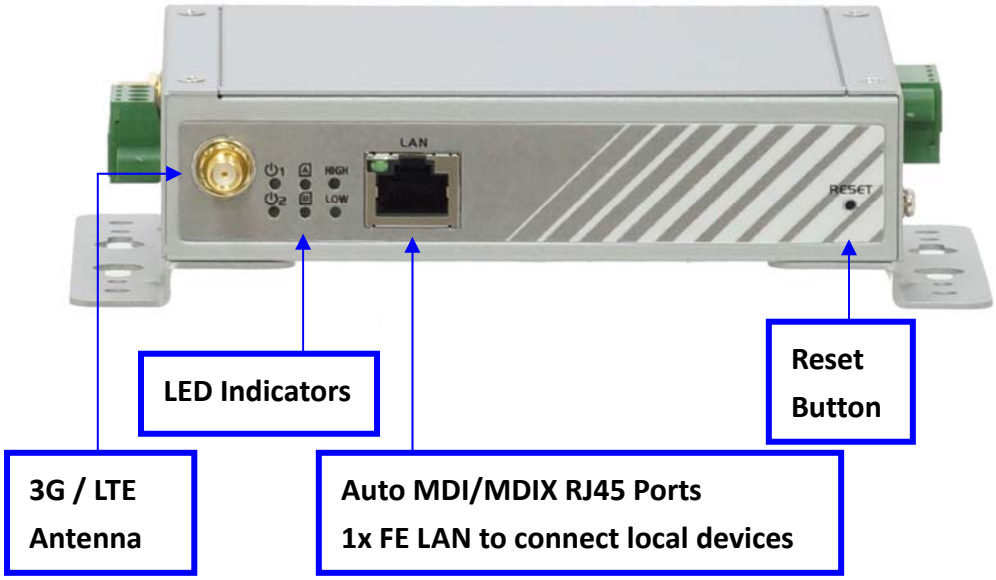
- Do not use the product in high humidity or high temperatures.
- Only use the power adapter that comes with the package. Using a different voltage rating power adaptor is dangerous and may damage the product.
- Do not open or repair the case yourself. If the product is too hot, turn off the power immediately and have it repaired at a qualified service center.
- Place the product on a stable surface and avoid using this product and all accessories outdoors.

1.2.2 SYSTEM REQUIREMENTS

Network Requirements	• 3G / 4G cellular service subscription • 10/100 Ethernet adapter on PC
Web-based Configuration Utility Requirements	**Computer with the following:** • Windows®, Macintosh, or Linux-based operating system • An installed Ethernet adapter **Browser Requirements:** • Internet Explorer 6.0 or higher • Chrome 2.0 or higher • Firefox 3.0 or higher • Safari 3.0 or higher
CD Installation Wizard Requirements	**Computer with the following:** • Windows® 7, Vista®, or XP with Service Pack 2 • An installed Ethernet adapter • CD-ROM drive

1.2.3 Hardware Configuration

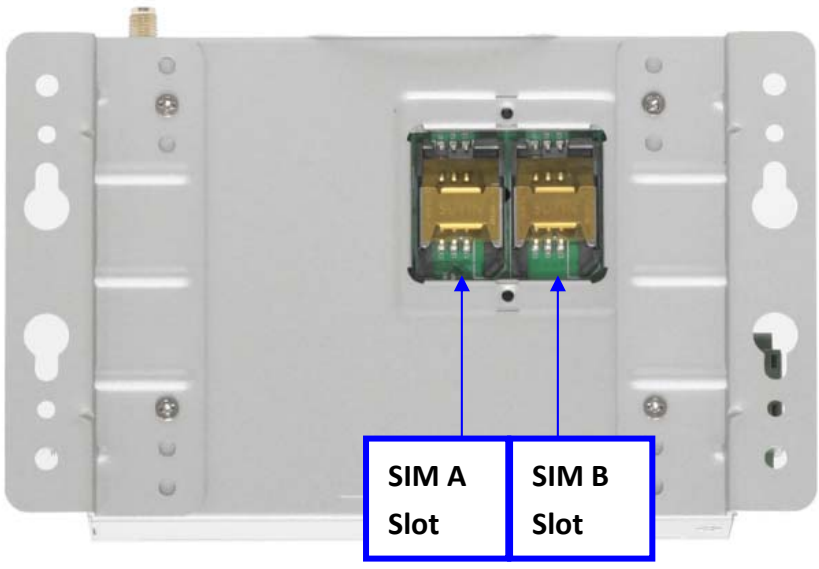
➢ Front View



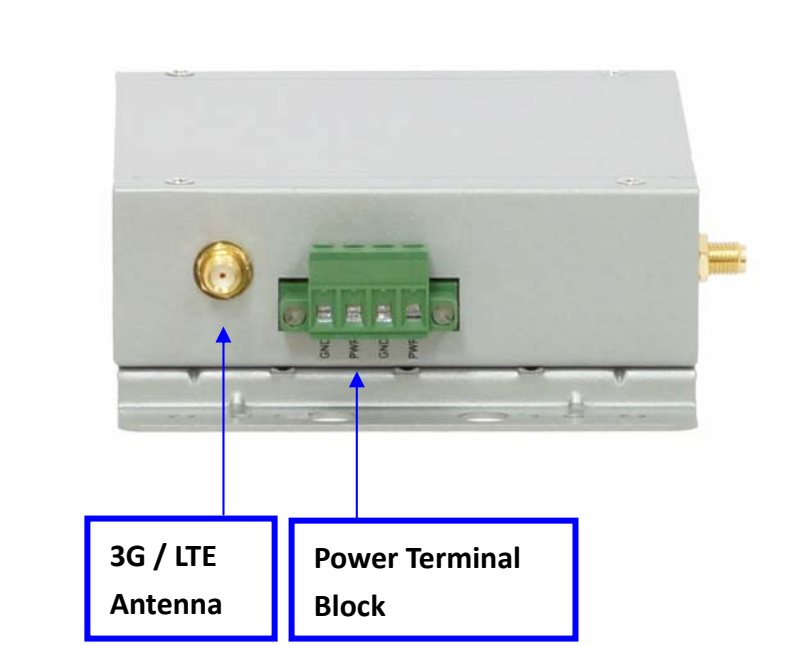
※Reset Button

The RESET button provides user with a quick and easy way to resort the default setting. Press the RESET button continuously for 6 seconds, and then release it. The device will restore to factory default settings.

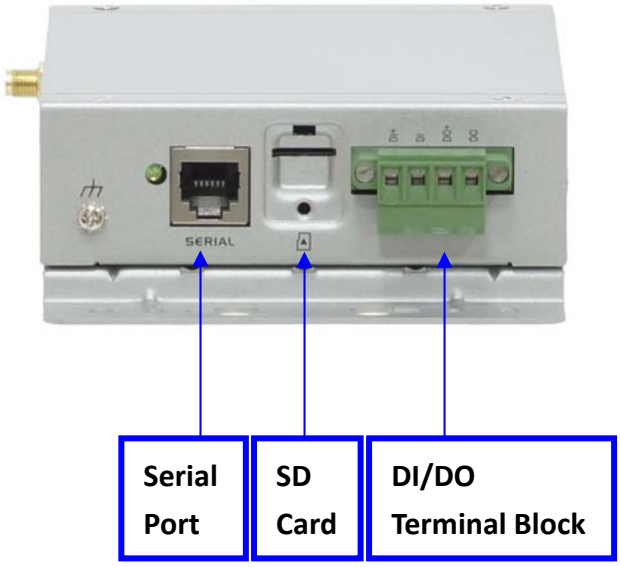
➢ Bottom View



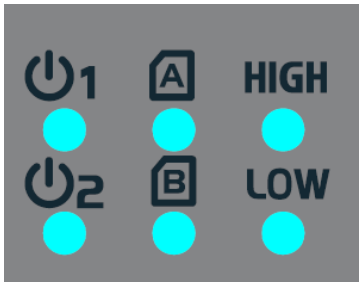
➢ Left View



➢ Right View



1.2.4 LED Indication



LED Icon	Indication	LED Color	Description
	Power Source 1	Green	**Steady ON:** Device is powered on by power source 1
	Power Source 2 (*[2])	Green	**Steady ON:** Device is powered on by power source 2
	SIM A (*[3])	Green	**Steady ON:** SIM card A is chosen for connection
	SIM B	Green	**Steady ON:** SIM card B is chosen for connection
HIGH	High Cellular Signal	Green	**Steady ON:** The signal strength of Cellular is strong
LOW	Low Cellular Signal	Green	**Steady ON:** The signal strength of Cellular is weak
	LAN	Green	**Steady ON:** Ethernet connection of LAN WAN is established **Flash:** Data packets are transferred
	Serial Port	Green	**Steady ON:** If serial device is attached

2 If both of power source 1 and power source 2 are connected, the device will choose power source 1 first. The LED of power source 2 will remain OFF at this condition.

3 The SIM LED indicates which SIM socket will be chosen for connection by system setting, no matter SIM card is inserted or not.

Chapter 2 Getting Started

This chapter describes how to install and configure the hardware and how to use the setup wizard to configure the network with the web GUI of GEM-2M series.

2.1 Hardware Installation

2.1.1 Mount the Unit

The GEM-2M series can be placed on a desktop, mounted on the wall or mounted on a DIN-rail. The DIN-rail bracket is not screwed on the product when out of factory. Please screw the DIN-rail bracket on the product first if necessary.

2.1.2 Insert the SIM Card

WARNNING: BEFORE INSERTING OR CHANGING THE SIM CARD, PLEASE MAKE SURE THAT POWER OF THE DEVICE IS SWITCHED OFF.

The SIM card slots are located at the bottom side of GEM-2M series housing in order to protect the SIM card. You need to unscrew and remove the outer SIM card cover before installing or removing the SIM card. Please follow the instructions to insert a SIM card. After SIM card is well placed, screw back the outer SIM card cover.

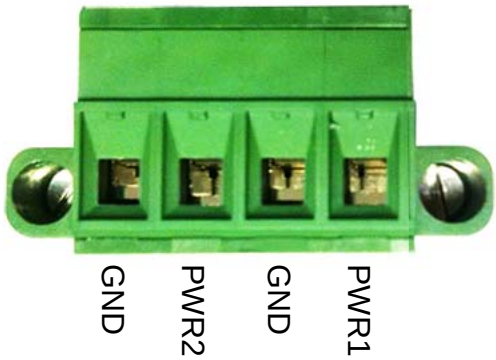
Step 1:
Follow red arrow to unlock SIM socket

Step 2:
Lift up SIM holder, and insert SIM card

Step 3:
Put back SIM holder, and follow red arrow to lock SIM socket

2.1.3 Connecting Power

The GEM-2M series can be powered by connecting one or two power sources to the terminal block. **It supports dual 9 to 48VDC power inputs**[4]. Following picture is the power terminal block pin assignments and it is located at the right side of device. Please check carefully and connect to the right power requirements and polarity.



There are a DC converter and a DC12V/2A power adapter[5] in the package for you to easily connect DC power adapter to this terminal block.

4 If both of power source 1 and power source 2 are connected, the device will choose power source 1 first. If power outage occurred from power source 1, this device will switch to power source 2 automatically and seamlessly.

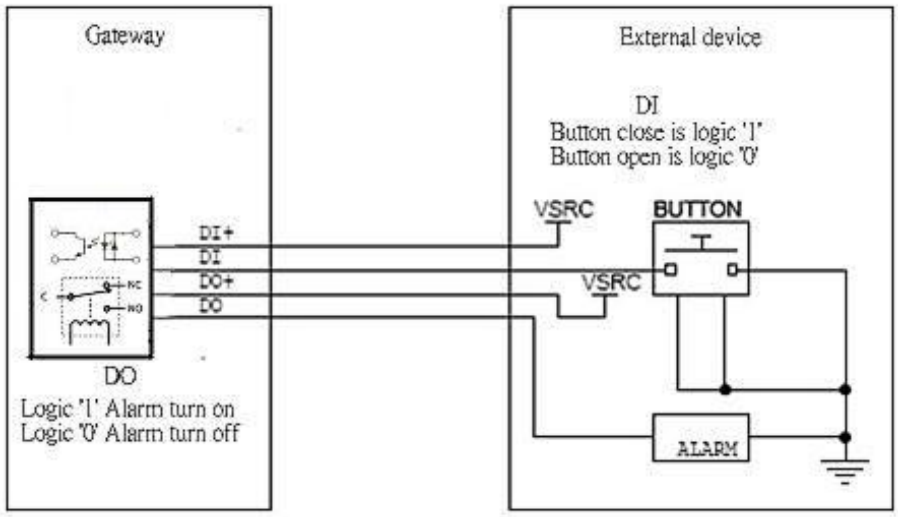
5 The maximum power consumption of GEM-2M series is 15.6W.

2.1.4 Connecting DI/DO Devices

There are a DI and a DO ports together with locating at the left side of device. Please refer to following specification to connect DI and DO devices.

Mode	Specification	
Digital Input	Trigger Voltage (high)	Logic level 1: 5V~30V
	Normal Voltage (low)	Logic level 0: 0V~2.0V
Digital Output	Voltage (Relay Mode)	Depends on external device maximum voltage is 30V
	Maximum Current	1A

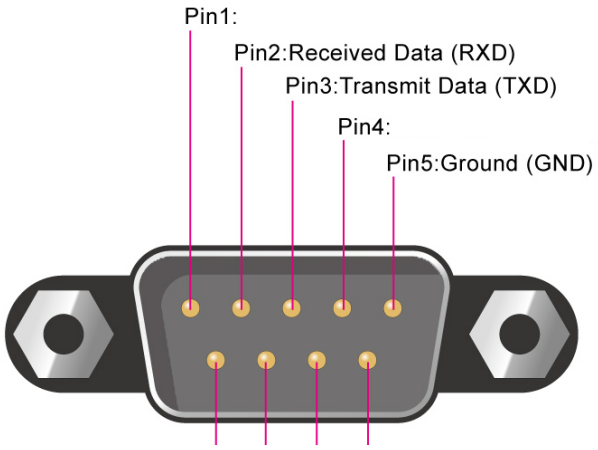
Example of Connection Diagram



2.1.5 Connecting Serial Devices

The GEM-2M provides one standard serial port RJ12 female connector and one RJ12 to DB9 conversion cable. Connect the serial device to the unit DB9 male port with the right pin assignments of RS-232/485 are shown as below.

RS232 Pinout



	Pin1	Pin2	Pin3	Pin4	Pin5	Pin6	Pin7	Pin8	Pin9
RS-232		RXD	TXD		GND				
RS-485		DATA-	DATA+		GND				

2.1.6 Connecting to the Network or a Host

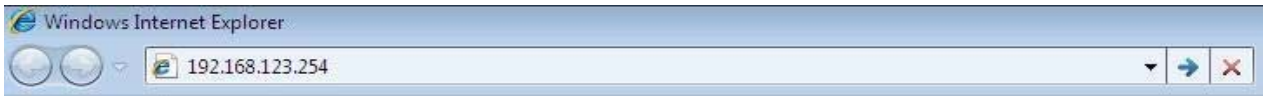
The GEM-2M series provides one RJ45 port to connect 10/100Mbps Ethernet. It can auto detect the transmission speed on the network and configure itself automatically. Connect one Ethernet cable to the RJ45 port (LAN) of the device on the front panel and plug another end of the Ethernet cable into your computer's network port. In this way, you can use the RJ45 Ethernet cable to connect the GEM-2M series to the host PC's Ethernet port for configuring or troubleshooting the device.

2.2 Easy Setup by Configuring WEB UI

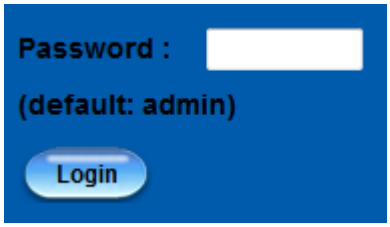
You can browse web UI to configure the device.

Browse to Activate the Setup Wizard

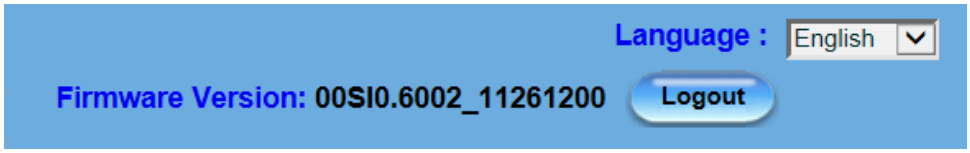
Type in the IP Address (**http://192.168.123.254**)[6]



When you see the login page, type the password **'admin'** [7] and then click **'Login'** button.



After logging in, select your **language** from the "Language" list. The user manual uses "English" for the illustration of all functions in the device.



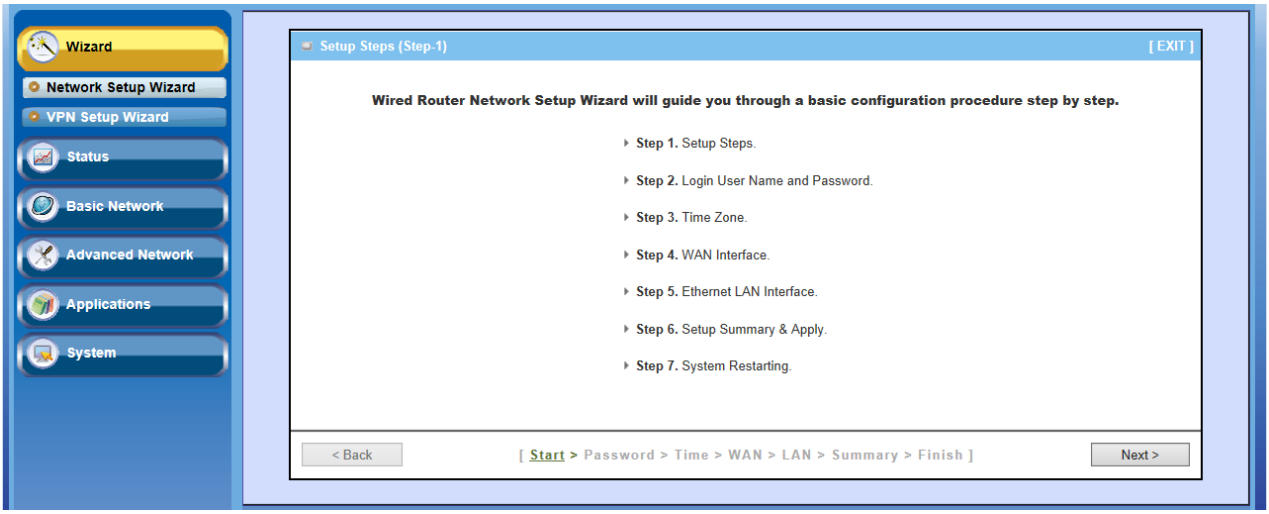
2.2.1 Wizard

Select **"Wizard"** for basic network settings and VPN settings in a simple way. Or, you can go to **Basic Network / Advanced Network / Applications / System** to setup the configuration by your own selection.

---

6 The default LAN IP address of this gateway is 192.168.123.254. If you change it, you need to type the new IP address

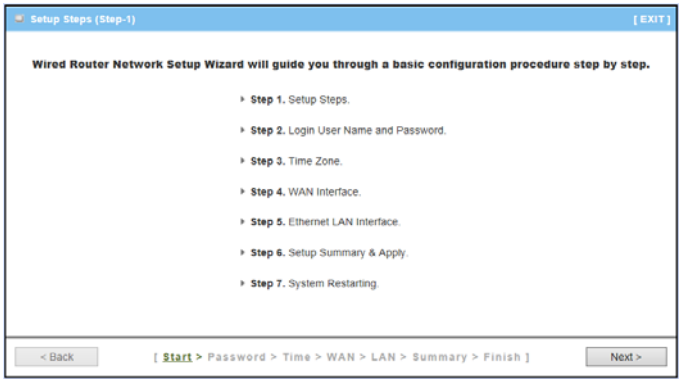
7 It's strongly recommending you to change this login password from default value


Wizard
Network Setup Wizard
VPN Setup Wizard
Status
Basic Network
Advanced Network
Applications
System
Setup Steps (Step-1)
[EXIT]
Wired Router Network Setup Wizard will guide you through a basic configuration procedure step by step.
Step 1. Setup Steps.
Step 2. Login User Name and Password.
Step 3. Time Zone.
Step 4. WAN Interface.
Step 5. Ethernet LAN Interface.
Step 6. Setup Summary & Apply.
Step 7. System Restarting.
< Back
[Start > Password > Time > WAN > LAN > Summary > Finish]
Next >

2.2.1.1 Configure with the Network Setup Wizard

Step 1: Guideline

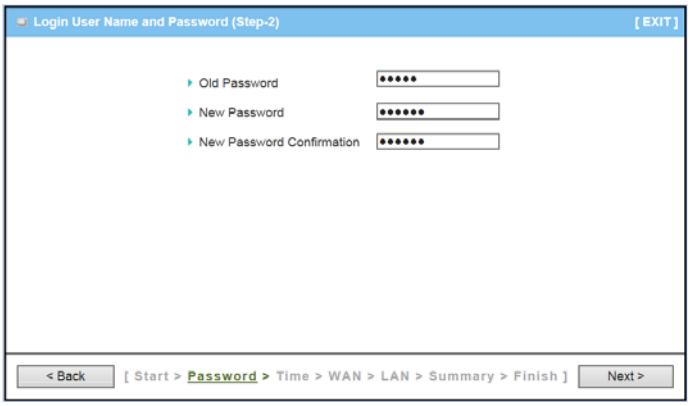
The network setup wizard will guide you to finish some basic settings, including login password, time zone, WAN interface and Ethernet LAN interface. One “EXIT” button at the upper-right corner of each window is provided for you to quit the setup process.


Setup Steps (Step-1)
[EXIT]
Wired Router Network Setup Wizard will guide you through a basic configuration procedure step by step.
Step 1. Setup Steps.
Step 2. Login User Name and Password.
Step 3. Time Zone.
Step 4. WAN Interface.
Step 5. Ethernet LAN Interface.
Step 6. Setup Summary & Apply.
Step 7. System Restarting.
< Back
[Start > Password > Time > WAN > LAN > Summary > Finish]
Next >

Press **“Next”** to start the wizard.

Step 2: Change Password

Password Configuration: You can change the login password of Web UI here. It’s strongly recommending you to change this login password from default value.

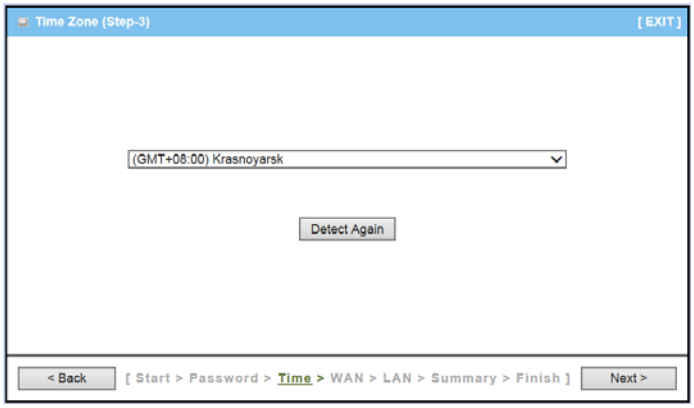

Login User Name and Password (Step-2)
[EXIT]
Old Password
New Password
New Password Confirmation
< Back
[Start > Password > Time > WAN > LAN > Summary > Finish]
Next >

Press **“Next”** to continue.

Step 3: Time Zone

Time Zone Configuration: It will detect your time zone automatically. If the result of auto detection is not correct, you can press “Detect Again” button or select manually.

Press **“Next”** to continue.



Step 4: WAN Interface

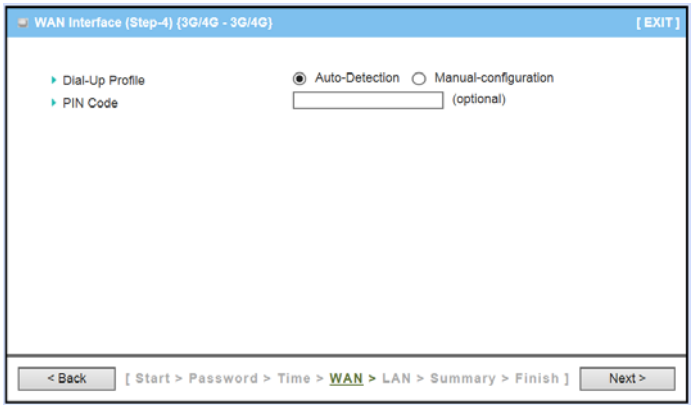
WAN Interface Configuration: Choose the physical interface and WAN type for Internet connection. Because the device provides only 3G/4G physical interface, and the only WAN type for the interface is also named as 3G/4G. Leave them be without change.

Press **“Next”** to continue.

Step 4-1: 3G/4G WAN Type

Since the only WAN interface is 3G/4G, please make sure you have inserted one or two SIM cards. If not, please power off this gateway, and insert SIM cards first. Then you can select “Auto-Detection” to finish dial-up profile automatically.

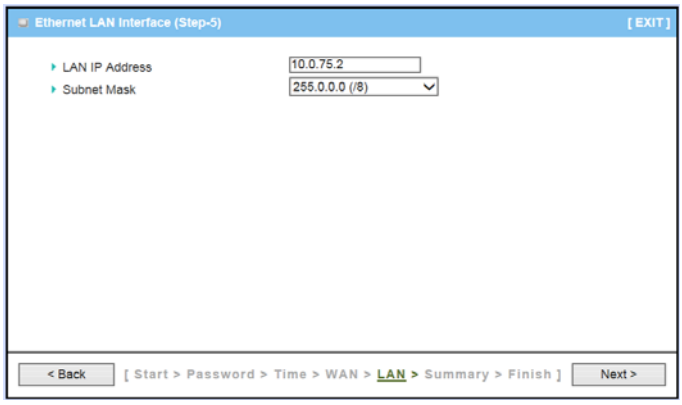
Press **“Next”** to continue.



Step 5: Ethernet LAN Interface

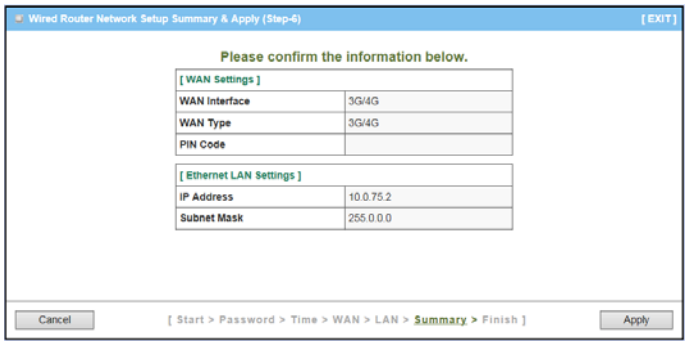
LAN Interface Configuration: Change the LAN IP address and subnet mask of this gateway for the Intranet. You can keep the default setting and go to next step.

Press **"Next"** to continue.



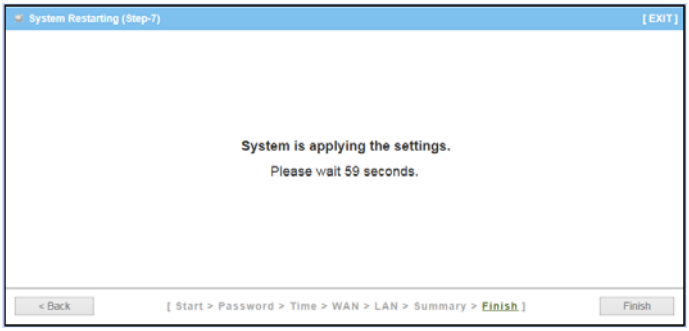
Step 6: Confirm and Apply

Check the new settings again. If all information is correct, please press "Apply" button to save new settings. Then it will take 65 seconds to restart this gateway and take new settings effective.


Wired Router Network Setup Summary & Apply (Step-6)
[EXIT]
Please confirm the information below.
[WAN Settings]
WAN Interface 3G/4G
WAN Type 3G/4G
PIN Code
[Ethernet LAN Settings]
IP Address 10.0.75.2
Subnet Mask 255.0.0.0
Cancel
[Start > Password > Time > WAN > LAN > Summary > Finish]
Apply

Step 7: Counting Down

Configuration is completed. Press "Finish" button to close Setup Wizard and browser counts down for 65 seconds and provides you with "Click here" button to reconnect to the device.

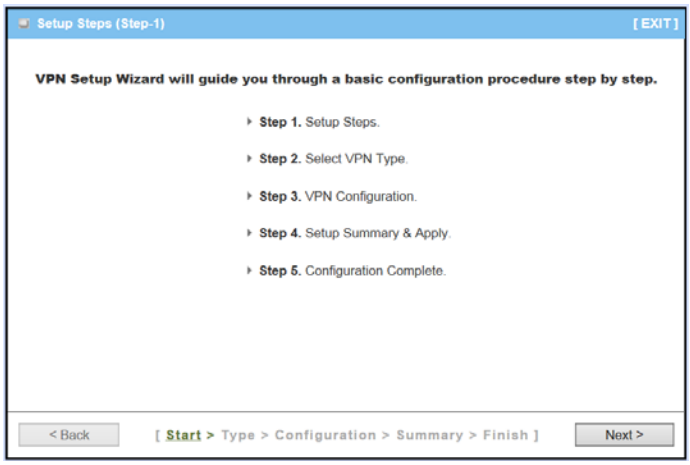

System Restarting (Step-7)
[EXIT]
System is applying the settings.
Please wait 59 seconds.
< Back
[Start > Password > Time > WAN > LAN > Summary > Finish]
Finish

2.2.1.2 Configure with the VPN Setup Wizard

Step 1: Guideline

The VPN setup wizard will guide you to finish profiles of IPSec, PPTP, L2TP and GRE VPN connection quickly.

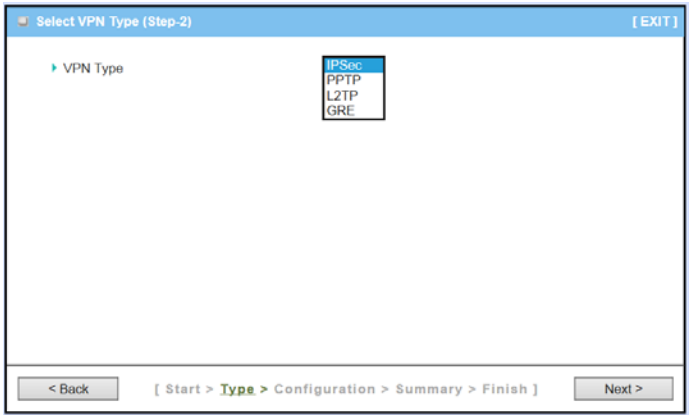
Press **"Next"** to start the wizard.


Setup Steps (Step-1)
[EXIT]
VPN Setup Wizard will guide you through a basic configuration procedure step by step.
Step 1. Setup Steps.
Step 2. Select VPN Type.
Step 3. VPN Configuration.
Step 4. Setup Summary & Apply.
Step 5. Configuration Complete.
< Back
[Start > Type > Configuration > Summary > Finish]
Next >

Step 2: VPN Type

Select type of VPN connection you want to create. Here you can choose IPSec, PPTP, L2TP or GRE.

Press **"Next"** to continue.

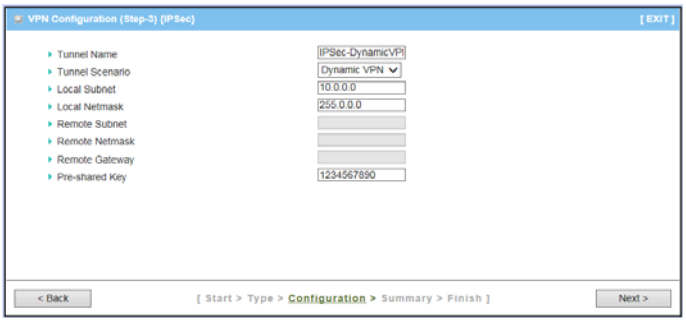


Step 3-1: IPSec

If choosing IPSec, there are five options of tunnel scenario can be chosen. "Site to Site" is for two offices to create a VPN tunnel. "Site to Host" is for one office to access one specific server via an IPSec tunnel. "Host to Site" is for service agents in the device to access the Intranet of an remote office via a tunnel. "Host to Host" is for two agent peers to create a secure tunnel for data communication. "Dynamic VPN" is for mobile users with dynamic IP address to connect to central office. For other options, please go to **[Advanced Network]-[VPN]** to setup. And then input the required network information and pre-shared key for VPN connection.

For Dynamic VPN, you don't need to input network information of remote subnet and remote gateway.

Press **"Next"** to continue.



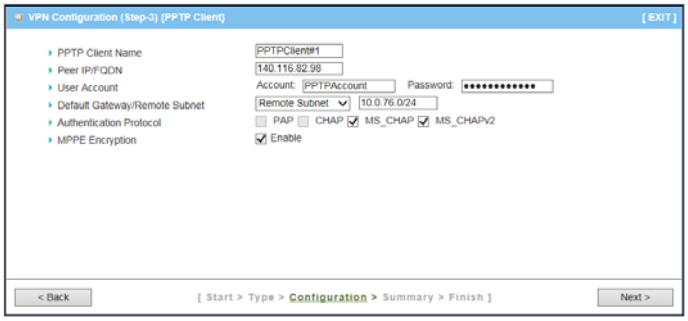
Step 3-2: PPTP

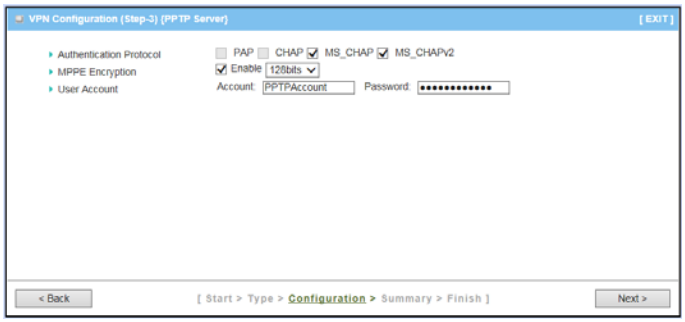
If choosing PPTP, there are two options of mode can be chosen. Choose "Client" if you want this device to connect to another PPTP server. Or choose "Server" if you want other PPTP clients to connect to it.

Press **"Next"** to continue.

If choosing PPTP Client, please input tunnel name, IP/FQDN of PPTP server, user name & password, choose default gateway / remote subnet, authentication protocol and MPPE encryption option. Please make sure these settings are accepted by remote PPTP server. Otherwise, PPTP server will reject the connection.

Press **"Next"** to continue.





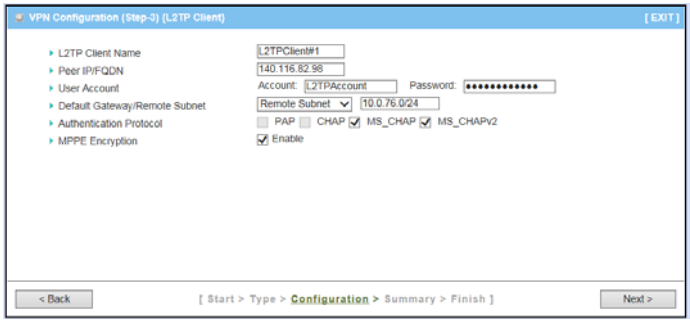
If choosing PPTP Server, please choose options of authentication protocol and key length of MPPE encryption. You also need to create a set of username and password for PPTP clients. In this wizard, you can only create one user account. If you want to create more user accounts, please go to **[Advanced Network]-[VPN]-[PPTP]** to add more users.

Press **"Next"** to continue.

Step 3-3: L2TP

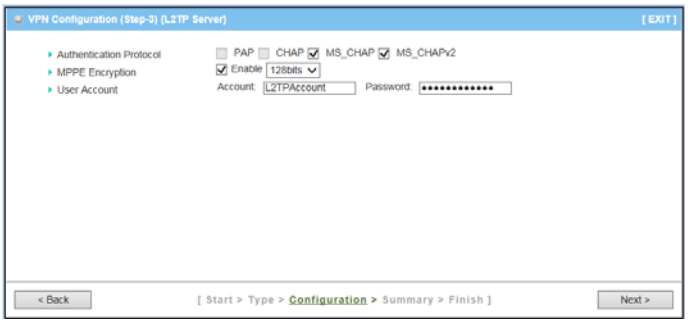
If choosing L2TP, there are two options of mode can be chosen. Choose "Client" if you want this device to connect to another L2TP server. Or choose "Server" if you want other L2TP clients to connect to it.

Press **"Next"** to continue.



If choosing L2TP Client, please input tunnel name, IP/FQDN of L2TP server, user name & password, choose authentication protocol and MPPE encryption option. Please make sure these settings are accepted by remote L2TP server. Otherwise, L2TP server will reject the connection.

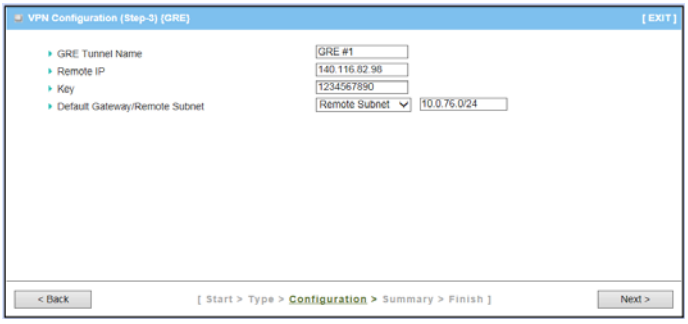
Press **"Next"** to continue.



If choosing L2TP Server, please choose options of authentication protocol and key length of MPPE encryption. You also need to create a set of username and password for L2TP clients. In this wizard, you can only create one user account. If you want to create more user accounts, please go to **[Advanced Network]-[VPN]-[L2TP]** to add more users.

Press **"Next"** to continue.

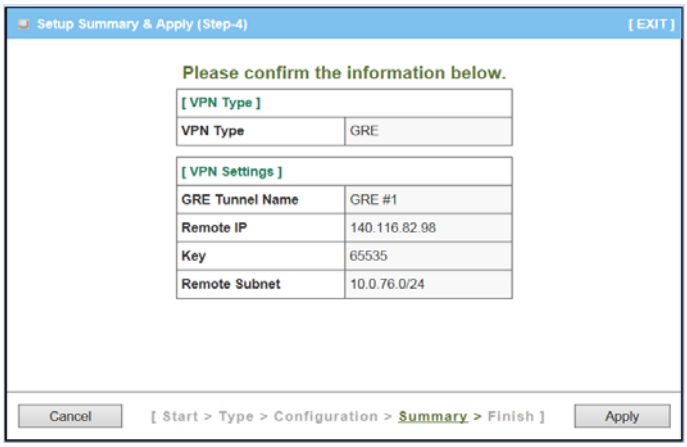
Step 3-4: GRE



If choosing GRE, please input tunnel name, IP address of remote GRE peer, Key ID and choose default gateway / remote subnet. Please make sure these settings are accepted by peer GRE site. Otherwise, remote GRE peer will reject the connection.

Press **"Next"** to continue.

Step 4: Confirm and Apply

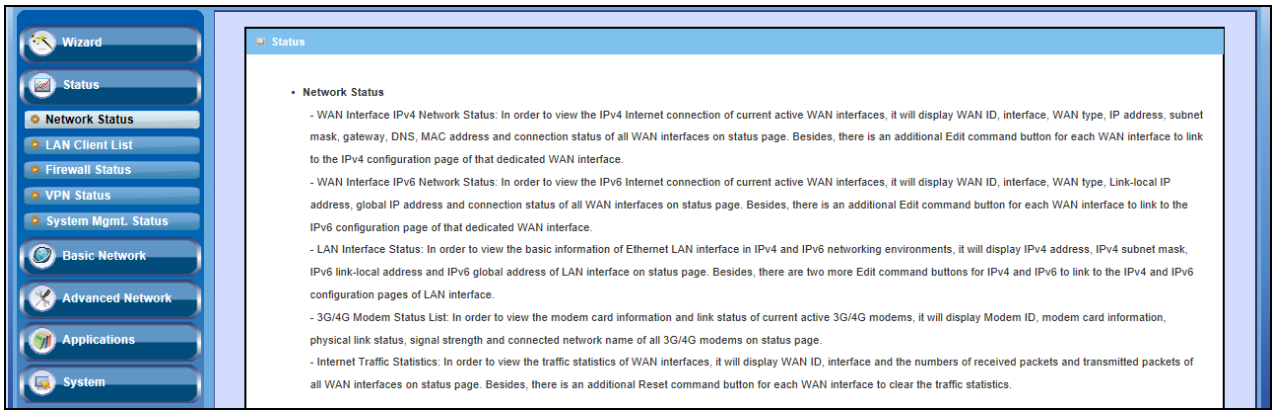


Confirm new settings. If all new settings are correct, please press "Apply" button to save these new settings and take them effective.

2.2.2 Status

There are 5 kinds of system status to be shown at this window. They are Network Status,

LAN Client List, Firewall Status, VPN Status and System Management Status.


Wizard
Status
Network Status
LAN Client List
Firewall Status
VPN Status
System Mgmt. Status
Basic Network
Advanced Network
Applications
System
Status
Network Status
- WAN Interface IPv4 Network Status: In order to view the IPv4 Internet connection of current active WAN interfaces, it will display WAN ID, interface, WAN type, IP address, subnet mask, gateway, DNS, MAC address and connection status of all WAN interfaces on status page. Besides, there is an additional Edit command button for each WAN interface to link to the IPv4 configuration page of that dedicated WAN interface.
- WAN Interface IPv6 Network Status: In order to view the IPv6 Internet connection of current active WAN interfaces, it will display WAN ID, interface, WAN type, Link-local IP address, global IP address and connection status of all WAN interfaces on status page. Besides, there is an additional Edit command button for each WAN interface to link to the IPv6 configuration page of that dedicated WAN interface.
- LAN Interface Status: In order to view the basic information of Ethernet LAN interface in IPv4 and IPv6 networking environments, it will display IPv4 address, IPv4 subnet mask, IPv6 link-local address and IPv6 global address of LAN interface on status page. Besides, there are two more Edit command buttons for IPv4 and IPv6 to link to the IPv4 and IPv6 configuration pages of LAN interface.
- 3G/4G Modem Status List: In order to view the modem card information and link status of current active 3G/4G modems, it will display Modem ID, modem card information, physical link status, signal strength and connected network name of all 3G/4G modems on status page.
- Internet Traffic Statistics: In order to view the traffic statistics of WAN interfaces, it will display WAN ID, interface and the numbers of received packets and transmitted packets of all WAN interfaces on status page. Besides, there is an additional Reset command button for each WAN interface to clear the traffic statistics.

2.2.2.1 Network Status

In Network Status page, you can review lots information of network status, including a connection diagram, WAN IPv4 status, WAN IPv6 status, LAN status, and 3G/4G modem status. You can also check the device time at the bottom of this page.

Connection Diagram

1. **3G/4G Icon:** Indicates if 3G/4G connection is established or not**.**
2. **Wired Client Icon:** Indicates how many Ethernet clients are connected now.

WAN Interface IPv4 Network Status

Display WAN type, IPv4 information, MAC information, and connection status of 3G/4G WAN interface in IPv4 networking. Press “Edit” button if you want to change settings.

WAN Interface IPv4 Network Status

WAN ID	Interface	WAN Type	IP Addr.	Subnet Mask	Gateway	DNS	MAC Address	Conn. Status	Actions
WAN-1	3G/4G	3G/4G	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0, 0.0.0.0	N/A	Connecting...	Edit

WAN Interface IPv6 Network Status

Display WAN type, IPv6 information, and connection status of 3G/4G WAN interface in IPv6 networking. Press “Edit” button if you want to change settings.

WAN Interface IPv6 Network Status						
WAN ID	Interface	WAN Type	Link-Local IP Address	Global IP Address	Connection Status	Actions
WAN-1		Disable				Edit

LAN Interface Status

Display IPv4 and IPv6 information of local network. Press “Edit” button if you want to change settings.

LAN Interface Status				
IPv4 Address	IPv4 Subnet Mask	IPv6 Link-Local Address	IPv6 Global Address	Actions
10.0.75.2	255.0.0.0		/64	Edit IPv4 / Edit IPv6

3G/4G Modem Status

Display modem information, link status, signal strength, and network (carrier) name of 3G/4G connection.

3G/4G Modem Status	Refresh				
Physical Interface	Card Information	Link Status	Signal Strength	Network Name	Actions
3G/4G	D18Q1	Connecting...	N/A	N/A	Detail

Internet Traffic Statistics

Display number of transmitted packets and received packets of 3G/4G WAN interface.

Internet Traffic Statistics			
WAN ID	Physical Interface	Received Packets	Transmitted Packets
WAN-1	3G/4G	0	0

Device Time

Display current time information of device.

Device Time: Fri, 02 Jan 1970 02:59:49 +0800

2.2.2.2 LAN Client List

In order to view the connection of current active wired clients, it will display LAN interface, IP address configuration, host name, MAC address and remaining lease time of all client devices on status page.

LAN Client List

LAN Interface	IP Address Configuration	Host Name	MAC Address	Remaining Lease Time
Ethernet	Dynamic / 10.0.75.100	JP-PC	20-6A-8A-5E-28-BF	23:49:13

2.2.2.3 Firewall Status

In Firewall Status page, you can review lots information of filter status, including Packet Filters, URL Blocking, Web Content Filters, MAC Control, Application Filters, IPS and other options of firewall.

Packet Filters

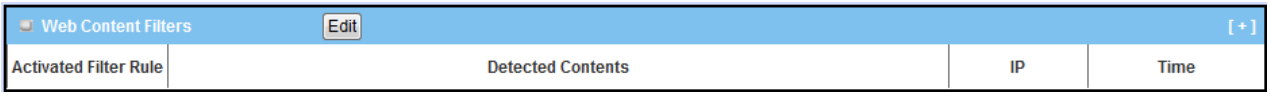
This window displays all detected contents of firing activated packet filter rules. One "Edit" button in the Packet Filters caption can let you change its settings. Another "[+]" or "[-]" button at the upper-right corner can unfold or fold the detected contents.

URL Blocking

This window displays all blocked URLs of firing activated URL blocking rules. One "Edit" button in the URL Blocking caption can let you change its settings. Another "[+]" or "[-]" button at the upper-right corner can unfold or fold the blocked URLs.

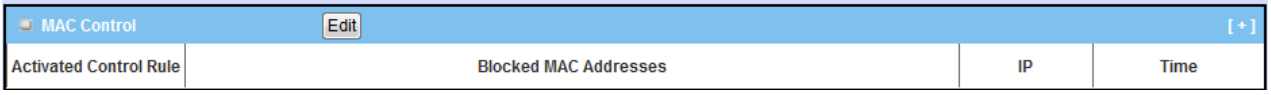
Web Content Filters

This window displays all detected contents of firing activated Web content filter rules. One "Edit" button in the Web Content Filters caption can let you change its settings. Another "[+]" or "[-]" button at the upper-right corner can unfold or fold the detected contents.



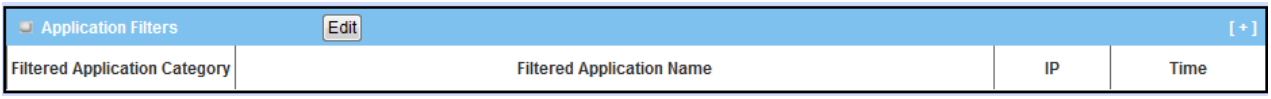
MAC Control

This window displays all blocked MAC addresses of firing activated MAC control rules. One "Edit" button in the MAC Control caption can let you change its settings. Another "[+]" or "[-]" button at the upper-right corner can unfold or fold the blocked MAC addresses.



Application Filters

This window displays all filtered applications of firing activated application filter rules. One "Edit" button in the Application Filters caption can let you change its settings. Another "[+]" or "[-]" button at the upper-right corner can unfold or fold the filtered applications.



IPS

This window displays all events of firing activated rules of IPS. One "Edit" button in the IPS caption can let you change its settings. Another "[+]" or "[-]" button at the upper-right corner can unfold or fold the intrusion events.

Options

Display option settings of firewall.

2.2.2.4 VPN Status

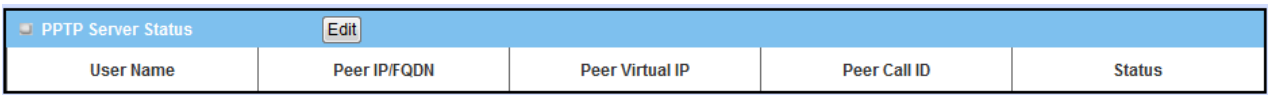
In VPN Status page, you can review lots information of VPN status, including IPSec status, PPTP Server status, PPTP Client status, L2TP Server status and L2TP Client status.

IPSec Status

Display the status of all activated tunnels of IPSec. One "Edit" button in the IPSec Status caption can let you change its settings.

PPTP Server Status

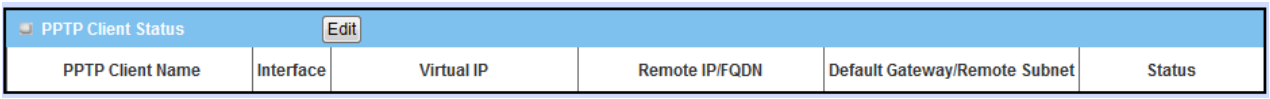
Display the status of all activated accounts of PPTP server. One "Edit" button in the PPTP Server Status caption can let you change its settings.



PPTP Client Status

Display the status of all activated PPTP clients. One "Edit" button in the PPTP Client Status

caption can let you change its settings.



L2TP Server Status

Display the status of all activated accounts of L2TP server. One "Edit" button in the L2TP Server Status caption can let you change its settings.

L2TP Client Status

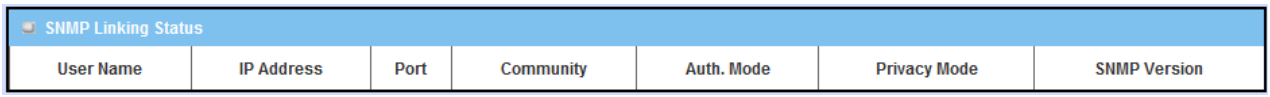
Display the status of all activated L2TP clients. One "Edit" button in the L2TP Client Status caption can let you change its settings.

2.2.2.5 System Management Status

In System Management Status page, you can review lots information of SNMP and TR-069 status.

SNMP Linking Status

Display information of SNMP linking.

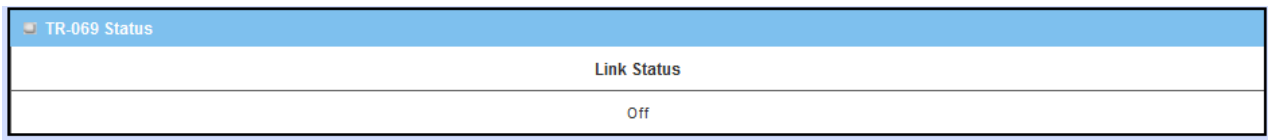


SNMP Trap Information

Display information of SNMP traps.

TR-069 Status

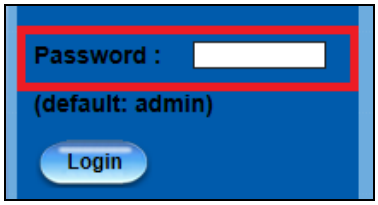
Display link status of TR-069.



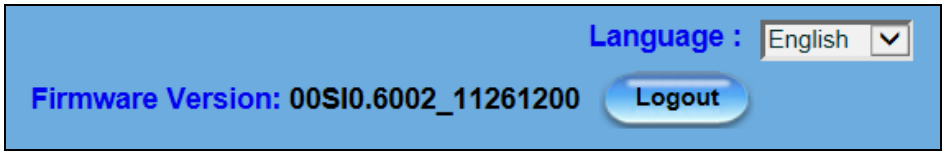
Chapter 3 Making Configurations

Whenever you want to configure your network or this device, you can access the Configuration Menu by opening the web browser and typing in the IP Address of the device. The default IP Address is: **192.168.123.254.** In the configuration section you may want to do Basic Network setup, Advanced Network setup, Applications setup or system-related setup and operations. These task buttons can be easily found in the cover page of the UI (User Interface).

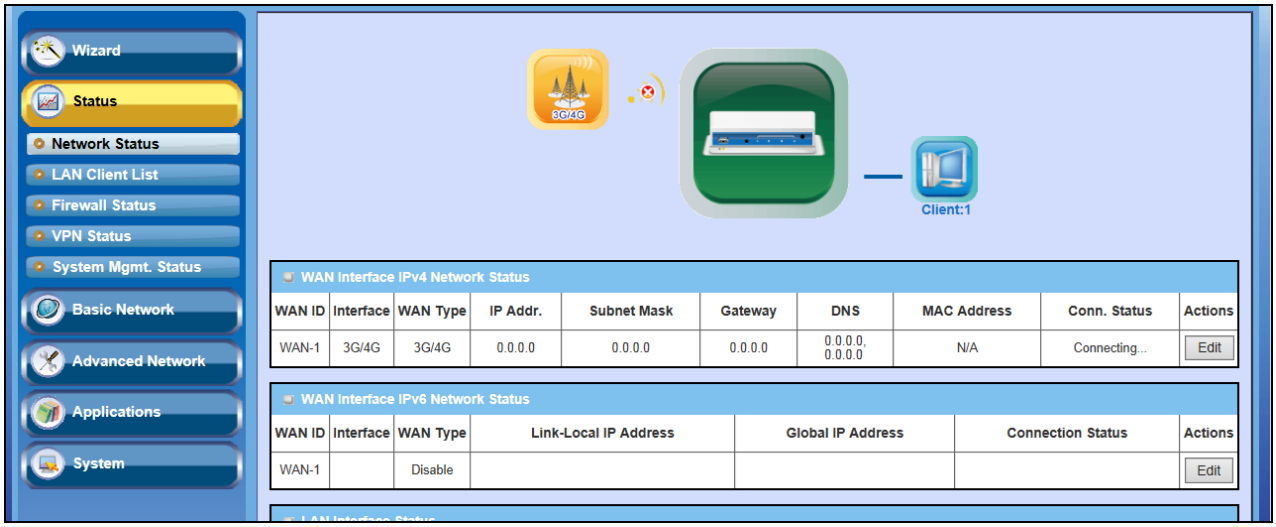
Enter the default password **"admin"** in the Password and then click **'Login'** button.



After login, select your **language** from the "Language" list. The user manual uses "English" for the illustration of all functions in the device.



Afterwards, you can go **Wizard, Basic Network, Advanced Network, Applications or System** respectively on left hand side of web page for device configuration.


Wizard
Status
Network Status
LAN Client List
Firewall Status
VPN Status
System Mgmt. Status
Basic Network
Advanced Network
Applications
System
3G/4G
Client:1
WAN Interface IPv4 Network Status
WAN ID | Interface | WAN Type | IP Addr. | Subnet Mask | Gateway | DNS | MAC Address | Conn. Status | Actions
WAN-1 | 3G/4G | 3G/4G | 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | 0.0.0.0, 0.0.0.0 | N/A | Connecting... | Edit
WAN Interface IPv6 Network Status
WAN ID | Interface | WAN Type | Link-Local IP Address | Global IP Address | Connection Status | Actions
WAN-1 | | Disable | | | | Edit

Note: *You can see the first screen is located at* ***[Status]-[Network Status]*** *after you logged in and the screen shows the Network Connection Status below.*

WAN Interface IPv4 Network Status

WAN ID	Interface	WAN Type	IP Addr.	Subnet Mask	Gateway	DNS	MAC Address	Conn. Status	Actions
WAN-1	3G/4G	3G/4G	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0, 0.0.0.0	N/A	Connecting...	Edit

WAN Interface IPv6 Network Status

WAN ID	Interface	WAN Type	Link-Local IP Address	Global IP Address	Connection Status	Actions
WAN-1		Disable				Edit

LAN Interface Status

IPv4 Address	IPv4 Subnet Mask	IPv6 Link-Local Address	IPv6 Global Address	Actions
10.0.75.2	255.0.0.0		/64	Edit IPv4 / Edit IPv6

3G/4G Modem Status Refresh

Physical Interface	Card Information	Link Status	Signal Strength	Network Name	Actions
3G/4G	D18Q1	Connecting...	N/A	N/A	Detail

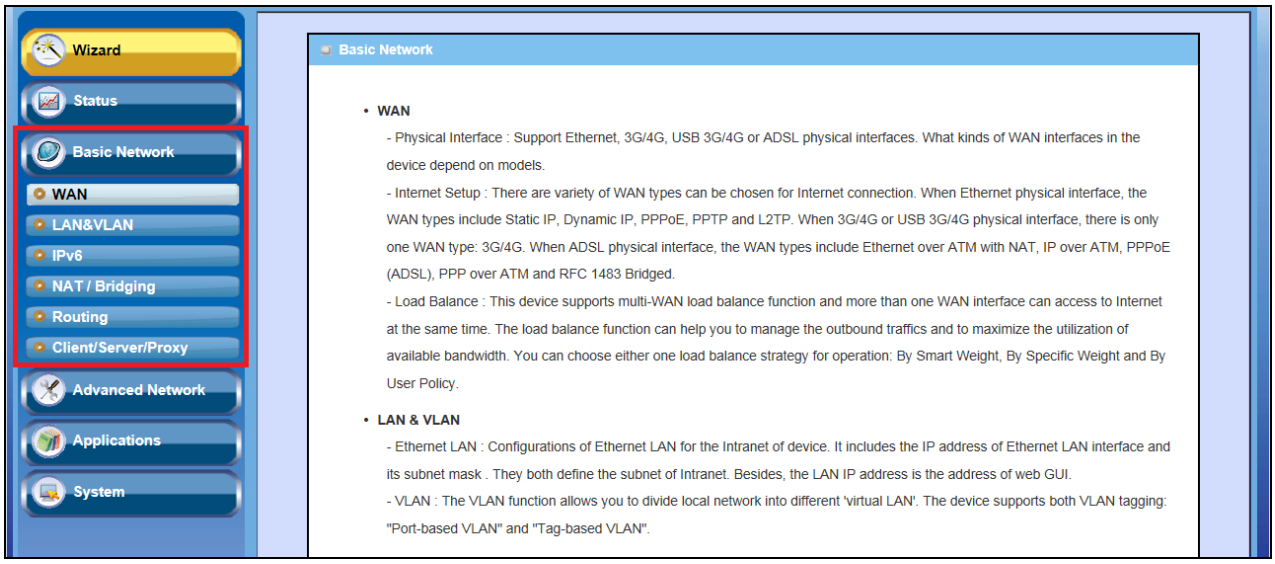
Internet Traffic Statistics

WAN ID	Physical Interface	Received Packets	Transmitted Packets
WAN-1	3G/4G	0	0

You can also check status of connected clients at **LAN Client List** page, and other advanced function status at **Firewall Status** page, **VPN Status** page and **System Management Status** page.

3.1 Basic Network

You can enter Basic Network for **WAN, LAN&VLAN, IPv6, NAT/Bridging, Routing, and Client/Server/Proxy** settings as the icon shown here.


Wizard
Status
Basic Network
WAN
LAN&VLAN
IPv6
NAT / Bridging
Routing
Client/Server/Proxy
Advanced Network
Applications
System
Basic Network
• WAN
- Physical Interface : Support Ethernet, 3G/4G, USB 3G/4G or ADSL physical interfaces. What kinds of WAN interfaces in the device depend on models.
- Internet Setup : There are variety of WAN types can be chosen for Internet connection. When Ethernet physical interface, the WAN types include Static IP, Dynamic IP, PPPoE, PPTP and L2TP. When 3G/4G or USB 3G/4G physical interface, there is only one WAN type: 3G/4G. When ADSL physical interface, the WAN types include Ethernet over ATM with NAT, IP over ATM, PPPoE (ADSL), PPP over ATM and RFC 1483 Bridged.
- Load Balance : This device supports multi-WAN load balance function and more than one WAN interface can access to Internet at the same time. The load balance function can help you to manage the outbound traffics and to maximize the utilization of available bandwidth. You can choose either one load balance strategy for operation: By Smart Weight, By Specific Weight and By User Policy.
• LAN & VLAN
- Ethernet LAN : Configurations of Ethernet LAN for the Intranet of device. It includes the IP address of Ethernet LAN interface and its subnet mask . They both define the subnet of Intranet. Besides, the LAN IP address is the address of web GUI.
- VLAN : The VLAN function allows you to divide local network into different 'virtual LAN'. The device supports both VLAN tagging: "Port-based VLAN" and "Tag-based VLAN".

3.1.1 WAN Setup

This device is equipped with one WAN Interface to support Internet connection. You can configure it to get proper connection setup.

3G/4G WAN: The gateway has one 3G/4G[8] modem built-in, please plug in SIM card and follow UI setting to setup.

Caution

- Please **MUST POWER OFF** the gateway before you insert or remove SIM card.
- It will damage SIM card if you insert or remove SIM card during gateway is in operation.
- Please follow instructions at section 2.1.2.

3.1.1.1 Physical Interface

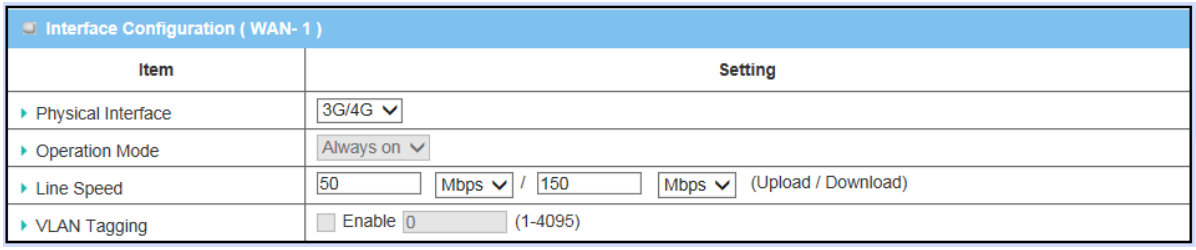
Click on the "**Edit**" button for the WAN interface and you can get the detail physical interface settings and then configure the settings as well. By default, the WAN-1 interface is forced to "**Always on**" mode, and operates as the primary internet connection.

Physical Interface List

Interface Name	Physical Interface	Operation Mode	Line Speed	Action
WAN-1	3G/4G	Always on	50 (Mbps) / 150 (Mbps)	Edit

8 The specification of embedded module depends on respective model.

1. **WAN-1**: The operation mode of first interface is forced to "**Always on**" mode, and operates as the primary Internet connection. You can click on the respective "**Edit**" button and configure the rest items for this interface.



1. **Physical Interface**: Select the WAN interface from the available list. For this gateway, there is only "3G/4G" physical interface for Internet connection. To use embedded 3G/4G modem to operate as the primary Internet connection (WAN-1), please configure it with following parameters.
2. **Operation Mode**: Since there is only one physical interface as primary WAN connection for the device, its operation mode must be "Always on".
3. **Line Speed**: You can specify the upstream / downstream speed (Mbps / Kbps) for the corresponding WAN connection. Such information will be referred in QoS function to manage the traffic load for each kind of services.
4. **VLAN Tagging**: If your ISP required a VLAN tag to be inserted into the WAN packets, you can enable this setting, and enter the specified tag value.

Afterwards, click on "Save" to store your settings or click "Undo" to give up the changes.

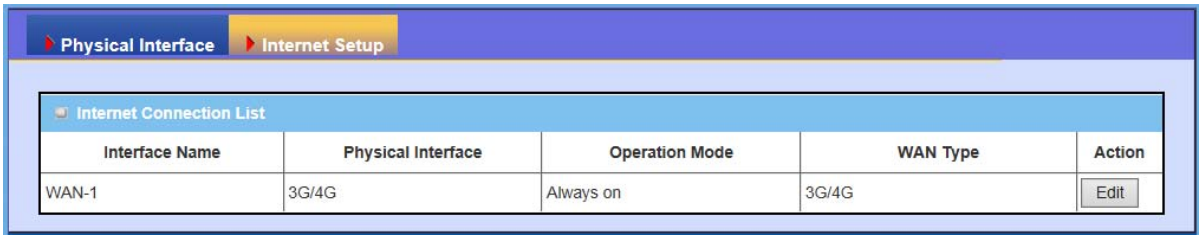
3.1.1.2 Internet Setup

There is only 3G/4G physical WAN interface in the device that you can configure it to get proper Internet connection setup. It supports only one WAN type to connect to Internet, 3G/4G. For 3G/4G WAN type, the ISP is a mobile operator that can provide LTE, HSPA+, HSPA, WCDMA, EDGE, GPRS data services[9]. And the device, attached with two SIM cards, can supports Dual-SIM failover mechanism for uninterrupted Internet connection.

Hereafter are some details of 3G/4G WAN type configuration:

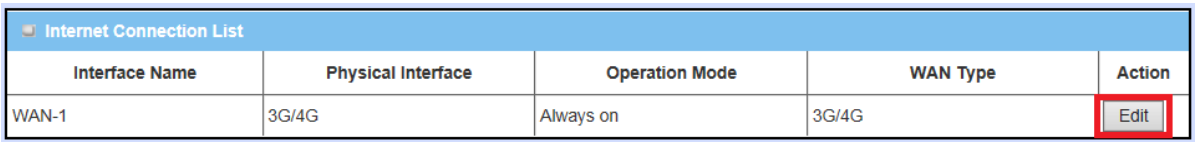
9 Different models have different specifications of embedded 3G module. Please refer to specification file for details.

3G/4G: If you have subscribed 3G/LTE data services from mobile operators. This gateway can support LTE/3G/2G depends on respective specifications. However, if your 3G data plan is not with a flat rate, it's recommended to set Connection Control mode to Connect-on-demand or Manually.



3.1.1.2.1 3G/4G WAN – 3G/4G

Click on the "**Edit**" button for the 3G/4G WAN interface and you can get the detail WAN settings and then configure the settings as well.

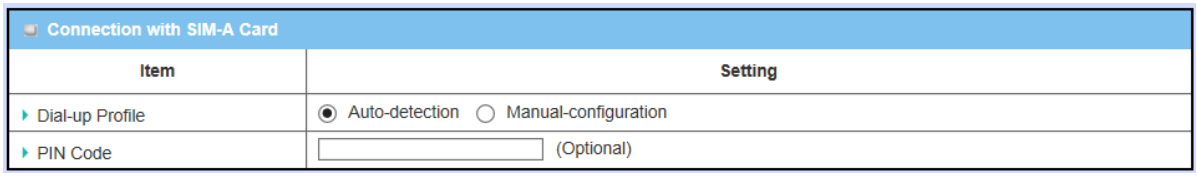


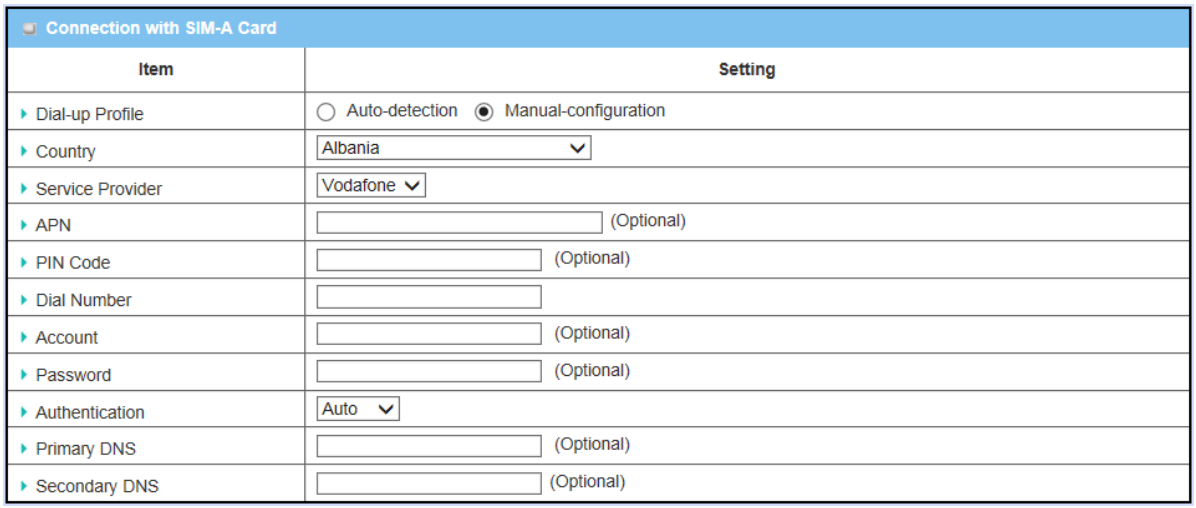
1. **WAN Type**: Leave it be "3G/4G".

1. **Preferred SIM Card**: Choose "SIM-A First", "SIM-B First", "SIM-A Only" or "SIM-B Only" for 3G/4G connection. There are two SIM card slots on this gateway and with four kinds of SIM card usage scenarios, including "SIM-A First", "SIM-B First", "SIM-A Only" and "SIM-B Only". By default, "SIM-A First" scenario is used to connect to mobile system for data transferring. If using "SIM-A First" scenario, the gateway will try to connect to the Internet by using SIM-A card first. And when the connection is broken, gateway system will switch to use SIM-B card for an alternate automatically. System will not switch back to use SIM-A card unless SIM-B connection is also broken. That is, SIM-A and SIM-B are used iteratively, but either one will keep being used for data transferring when current connection is still alive. In the same way, the gateway will try to connect to the

Internet by using SIM-B card first if choosing “SIM-B First”. However, when “SIM-A Only” or “SIM-B Only” is used, that means the specified SIM slot of card is the ONLY one to be used for negotiation parameters between gateway device and mobile base station.

When you select “SIM-A First” or “SIM-A Only”, there will be a configuration window of "Connection with SIM-A Card" beneath the "3G/4G WAN Type Configuration" window. However, when you select “SIM-B First” or “SIM-B Only”, there will be a configuration window of "Connection with SIM-B Card" beneath the "3G/4G WAN Type Configuration" window. All configuration items are the same in SIM-A and SIM-B configuration. Furthermore, there is also a common configuration window for 3G/4G connection after "3G/4G WAN Type Configuration" window, "Connection with SIM-A Card" window and "Connection with SIM-B Card" window.



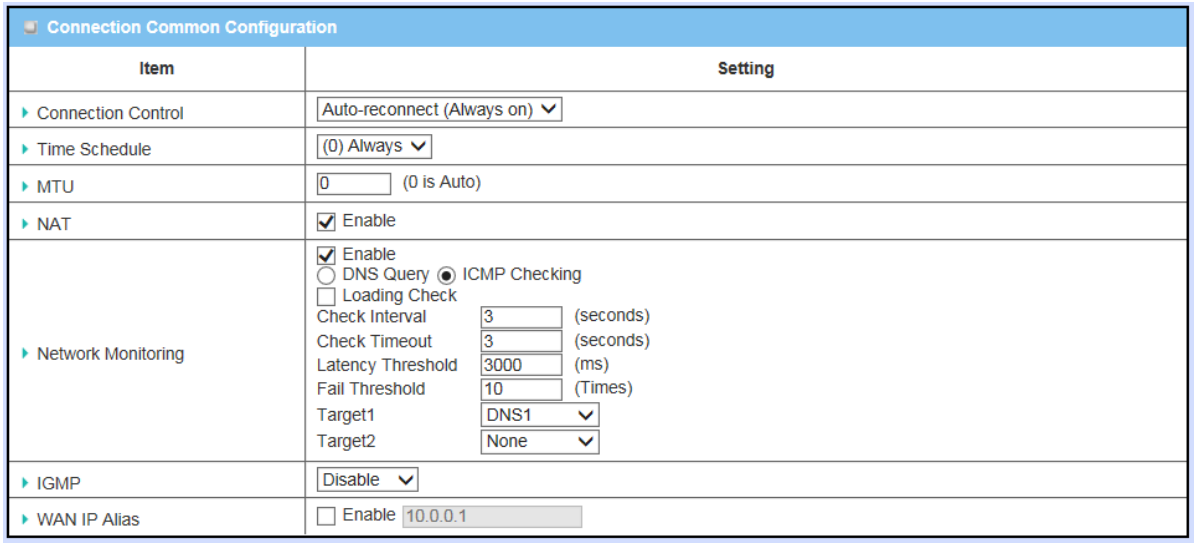


1. **Dial-up Profile:** After you subscribe 3G/4G data service, your operator will provide some information for you to setup connection, such as APN, dialed number, account or password. If you know this information exactly, you can choose “Manual-configuration” option and type in that information by your own. Otherwise, you can select “Auto-detection” to let this gateway detect automatically. Even you choose “Manual” setting, this gateway will show responding information for your reference to setup the dial-up profile after you

select country and service provider.

If you choose “SIM-A First” or “SIM-A Only” for Preferred SIM Card, you need to input dial-up profile for SIM-A. Similarly, you need to input dial-up profile for SIM-B when you choose “SIM-B First” or “SIM-B Only” as your preferred one.

2. **Country & Service Provider:** When you choose “Manual-configuration” option for the Dial-up Profile, you must select the country and service provider to retrieve related parameters from system for dialing up to connect to Internet. Once system doesn't store related parameters or stores not-matched parameters, you must specify them one by one manually.
3. **APN:** When you select the target country and service provider for manual dial-up profile, system will show related APN value. Change it if it is not correct for you.
4. **PIN Code:** Enter PIN code of SIM card if your SIM card needs it to unlock.
5. **Dial Number:** Enter the dialed number that is provided by your ISP.
6. **Account & Password:** Enter Account and Password that is provided by your ISP.
7. **Authentication:** Choose “Auto”, “PAP”, or “CHAP” according to your ISP’s authentication approach. Just keep it with “Auto” if you can’t make sure.
8. **Primary/Secondary DNS:** Enter IP address of Domain Name Server. You can keep them in blank, because most ISP will assign them automatically.



1. **Connection Control**: Select your connection control scheme from the drop list: “Auto-reconnect (Always on)”, “Dial-on-demand” or “Connect Manually”. If selecting “Auto-reconnect (Always on)”, this gateway will start to establish Internet connection automatically since it’s powered on. It’s recommended to

choose this scheme if for mission critical applications to ensure Internet connection is available all the time. If choosing “Dial-on-demand”, this gateway won’t start to establish Internet connection until local data is going to be sent to WAN side. During normal operation, this gateway will disconnect WAN connection if idle time reaches the value of "Maximum Idle Time". If choosing “Connect Manually”, this gateway won’t start to establish WAN connection until you press “Connect” button on web UI. During normal operation, this gateway will disconnect WAN connection if idle time reaches the value of "Maximum Idle Time".

2. **Time Schedule**: This option allows you to limit WAN connection available in a certain time period. You can select **“Always”** option or a time schedule object from the schedule object list that you can find them in **[System]-[Scheduling]**.
3. **MTU**: MTU refers to "Maximum Transmit Unit". Different WAN types of connection will have different value. You can leave it with 0 (Auto) if you are not sure about this setting.
4. **NAT:** By default, it is enabled. If you disable this option, there will be no NAT mechanism between LAN side and WAN side.
5. **Network Monitoring:** You can do preferred settings by using this feature to monitor the connection status of WAN interface. Checking mechanism depends on several parameters defined here. The network monitoring provides the WAN interface status and then system can prevent embedded 3G/LTE modem from some sort of auto-timeout and disconnects from the Internet after a period of inactivity.

   Enable: Check the box to do Network Monitoring. By default, it is checked.

   DNS Query/ICMP Checking: Do the keep alive through DNS query packets or ICMP packets.

   Loading Checking: The response time of replied keep-alive packets may increase when WAN bandwidth is fully occupied. To avoid keep-alive feature work abnormally, enable this option will stop sending keep-alive packets when there are continuous incoming and outgoing data packets passing through WAN connection. By default, the Loading Checking is enabled.

   Check Interval: Indicate how often to send keep-alive packet.

   Check Timeout: Set allowance of time period to receive response of keep-alive packet. If this gateway doesn’t receive response within this time period, this

gateway will record this keep alive is failed.

Latency Threshold: Set acceptance of response time. This gateway will record this keep-alive check is failed if the response time of replied packet is longer than this setting.

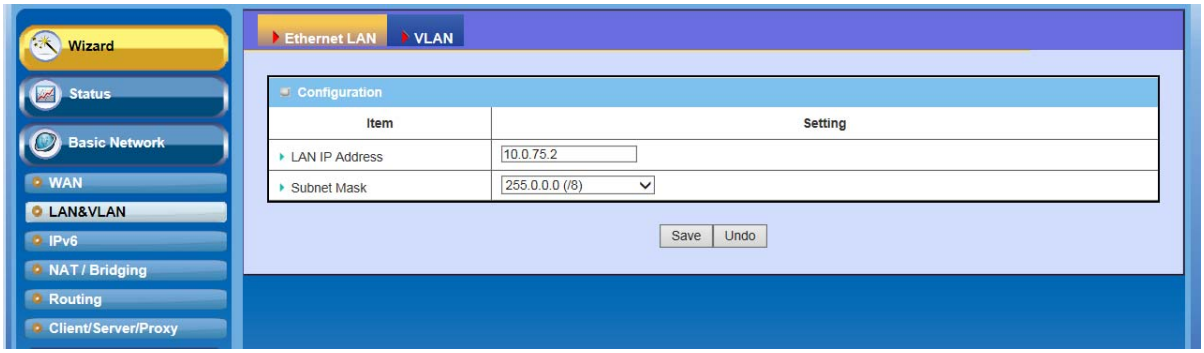
Fail Threshold: Times of failed checking. This WAN connection will be recognized as broken if the times of continuous failed keep-alive checking equals to this value.

Target1/Target2: Set host that is used for keep alive checking. It can be DNS1, DNS2, default Gateway, or other host that you need to input IP address manually.

6. **IGMP:** Enable or disable multicast traffics from Internet. You may enable as auto mode or select by the option list of IGMP v1, IGMP v2, IGMP v3 and Auto.
7. **WAN IP Alias:** The device supports 2 WAN IP addresses for a physical interface, one is for primary connection that provides users/devices in the LAN to access Internet; the other is a virtual connection that let remote user to manage this device.

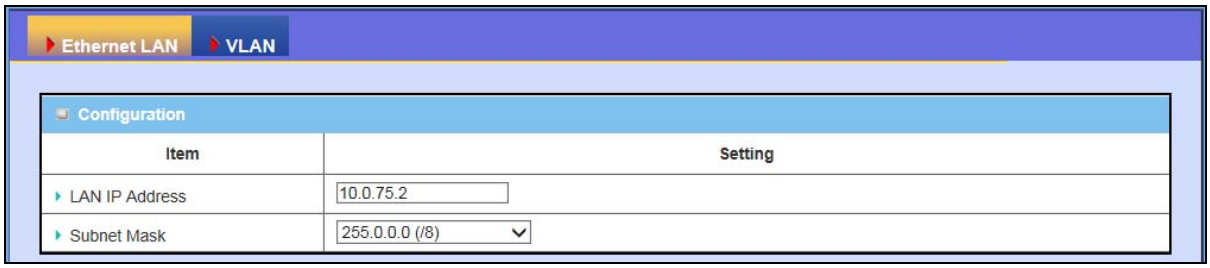
3.1.2 LAN & VLAN Setup

This device is equipped with one Fast Ethernet LAN port as to connect your local devices via Ethernet cables. Besides, VLAN function is provided to organize your local networks.

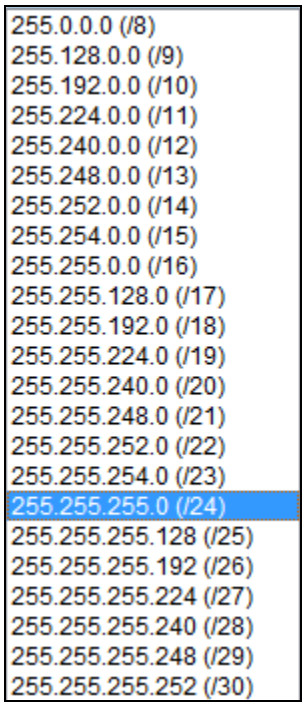


3.1.2.1 Ethernet LAN

Please follow the following instructions to do IPv4 Ethernet LAN Setup.



1. **LAN IP Address**: The local IP address of this device. The computers on your network must use the LAN IP address of this device as their Default Gateway. You can change it if necessary. It's also the IP address of web UI. If you change it, you need to type new IP address in the browser to see web UI. By default, LAN IP Address is 192.168.123.254.
2. **Subnet Mask:** Input your subnet mask. Subnet mask defines how many clients are allowed in one network or subnet. The default subnet mask is 255.255.255.0 (/24), and it means maximum 254 IP addresses are allowed in this subnet. However, one of them is occupied by LAN IP address of this gateway, so there are maximum 253 clients allowed in LAN network. Hereafter are the available options for subnet mask.



3.1.2.2 VLAN

This section provides a brief description of VLANs and explains how to create and modify virtual LANs which are more commonly known as VLANs. A VLAN is a logical network under a certain switch or router device to group lots of client hosts with a specific VLAN ID. This device supports both Port-based VLAN and Tag-based VLAN.

In Port-based VLAN, all client hosts belong to the same group by transferring data via some physical ports that are tagged with same VLAN ID in the device. The ports of a VLAN form an independent traffic domain in which the traffic generated by the nodes remains within the VLAN. However, in Tag-based VLAN, all packets with same VLAN ID will be treated as the same group of them and own same access property and QoS property. It is especially useful when individuals of a VLAN group are located at different floor location.

The VLAN function allows you to divide local network into different **"**virtual LANs". In some cases, ISP may need router to support "VLAN tag" for certain kinds of services (e.g. IPTV) to work properly. In some cases, SMB departments are separated and located at any floor of building. All client hosts in same department should own common access property and QoS property. You can select either one operation mode, port-based VLAN or tag-based VLAN, and then configure according to your network configuration.

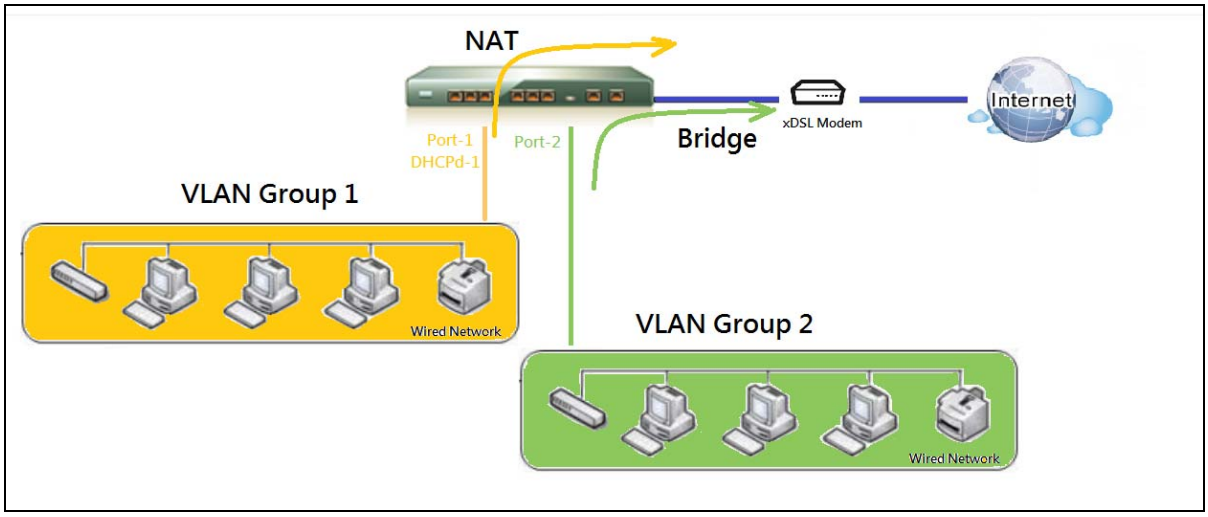
Please be noted, since there is only one physical Ethernet LAN port in the gateway, there is only little configuration if you choose the Port-based VLAN.

3.1.2.2.1 VLAN Scenarios

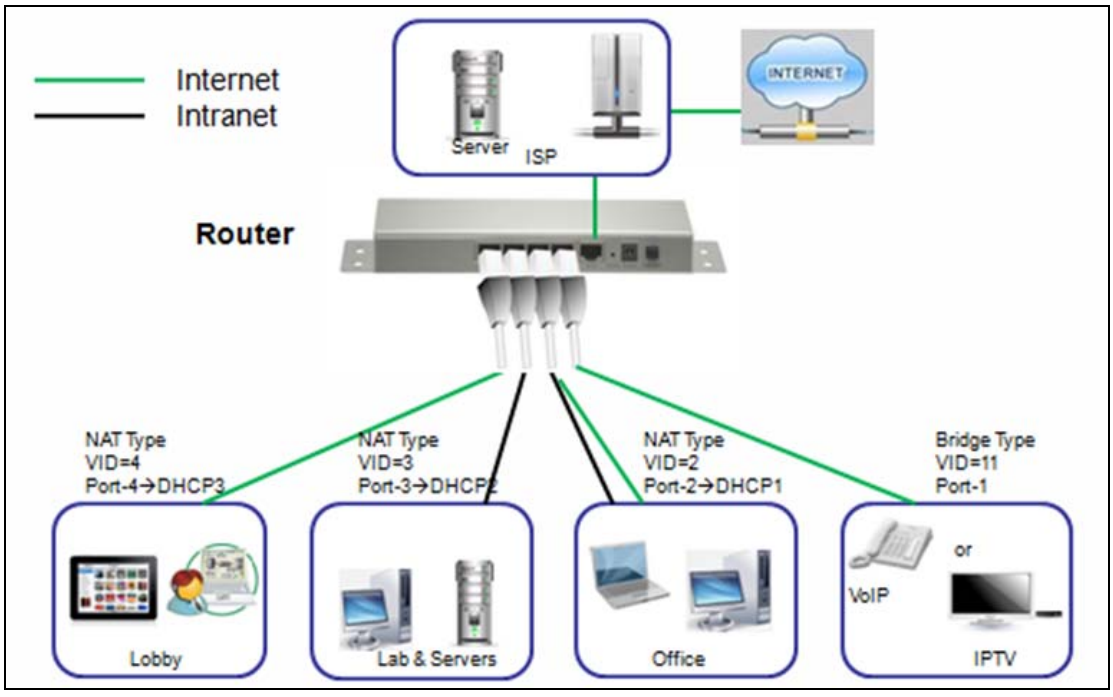
There are some common VLAN scenarios for the device as follows:

- Port-Based VLAN Tagging for Differentiated Services

Port-based VLAN function can group Ethernet ports together for differentiated services like Internet surfing, multimedia enjoyment, VoIP talking, and so on. Two operation modes, NAT and Bridge, can be applied to each VLAN group. One DHCP server is allocated for an NAT VLAN group to let group host member get its IP address. Thus, each host can surf Internet via the NAT mechanism of business access gateway. At bridge mode, Intranet packet flow was delivered out WAN trunk port with VLAN tag to upper link for different services.



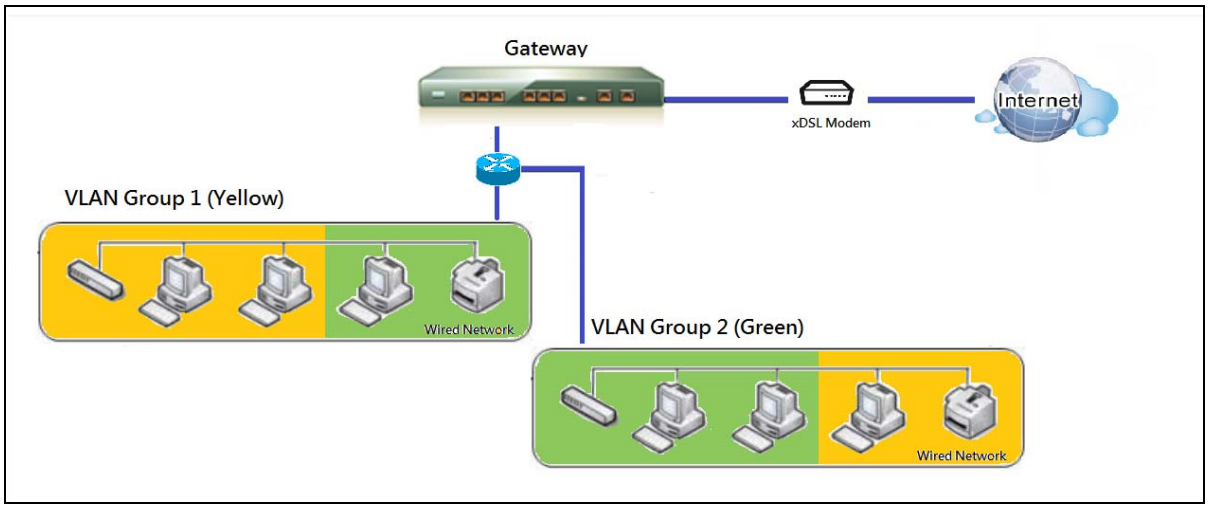
A port-based VLAN is a group of ports on an Ethernet of Wired Gateway that form a logical Ethernet segment. Following is an example. In SMB or a company, administrator schemes out 4 segments, Lobby, Lab & Servers, Office and VoIP & IPTV. In a Wireless Gateway, administrator can configure Lobby segment with VLAN ID 4. The VLAN group includes Port-4 with NAT mode and DHCP-3 server equipped. He also configure Lab & Servers segment with VLAN ID 3. The VLAN group includes Port-3 with NAT mode and DHCP-2 server equipped. However, he configure Office segment with VLAN ID 2. The VLAN group includes Port-2 with NAT mode and DHCP-1 server equipped. At last, administrator also configure VoIP & IPTV segment with VLAN ID 11. The VLAN group includes Port-1 with bridge mode to WAN interface as shown at following diagram.



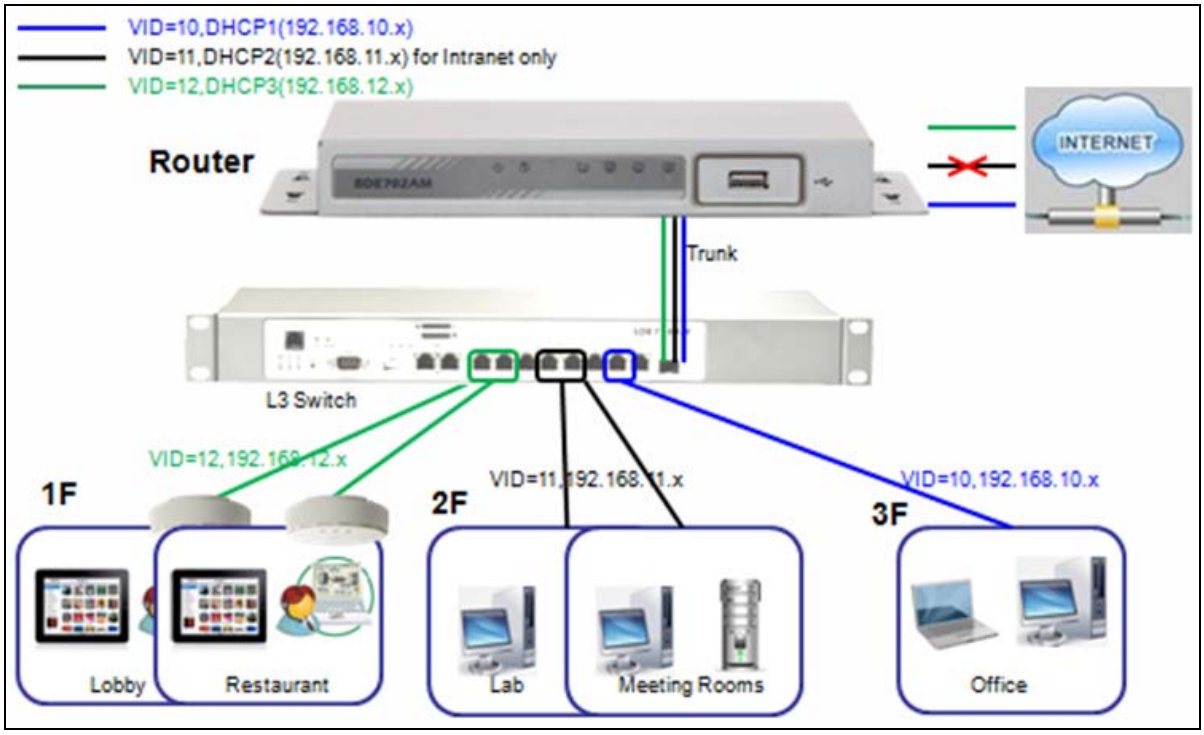
Above is the general case for 4 Ethernet LAN ports in the gateway. But the device has only one Ethernet LAN port and two different kinds of application for the Port-based VLAN tagging, NAT or Bridge.

- Tag-based VLAN Tagging for Location-free Departments

Tag-based VLAN function can specify some groups with different VLAN tags for deploying department subnets in Intranet. All packet flows can carry with different VLAN tags even at the same physical port for Intranet. These flows can be directed to different destination because they have differentiated tags. The approach is very useful to group some hosts in different geographic location to be the same department.



Tag-based VLAN is also called a VLAN Trunk. The VLAN Trunk collects all packet flows with different VLAN IDs from Router device and delivers them in the Intranet. VLAN membership in a tagged VLAN is determined by VLAN ID information within the packet frames that are received on a port. Administrator can further use a VLAN switch to separate the VLAN trunk to different groups based on VLAN ID. Following is an example. In SMB or a company, administrator schemes out 3 segments, Lobby & Restaurant, Lab & Meeting Rooms and Office. In a Security VPN Gateway, administrator can configure Lobby & Restaurant segment with VLAN ID 12. The VLAN group is equipped with DHCP-3 server to construct a 192.168.12.x subnet. He also configure Lab & Meeting Rooms segment with VLAN ID 11. The VLAN group is equipped with DHCP-2 server to construct a 192.168.11.x subnet for Intranet only. That is, any client host in VLAN 11 group can't access the Internet. However, he configures Office segment with VLAN ID 10. The VLAN group is equipped with DHCP-1 server to construct a 192.168.10.x subnet. In this example, VLAN 10 and 12 groups can access the Internet as following diagram.

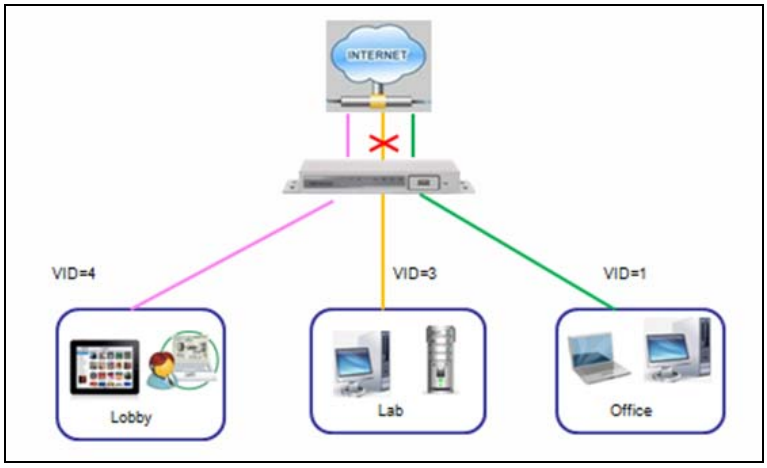


- VLAN Group Access Control

Administrator can specify the Internet access right for all VLAN groups. He also can configure which VLAN groups can communicate each other.

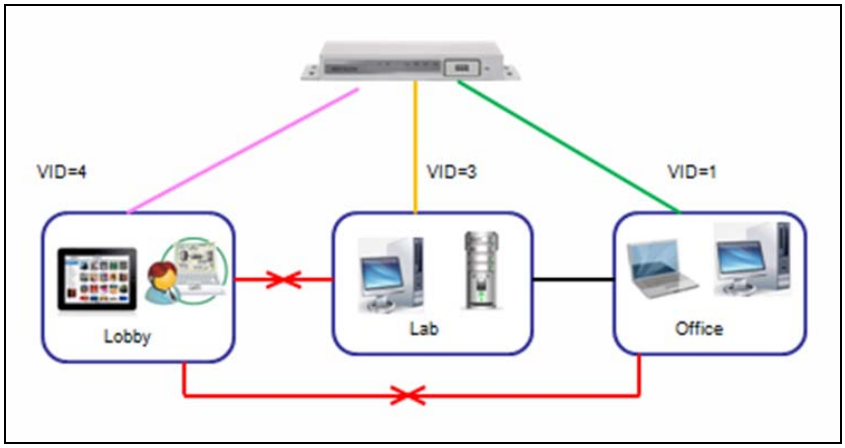
VLAN Group Internet Access

Administrator can specify members of one VLAN group to be able to access Internet or not. Following is an example that VLAN groups of VID is 1 and 4 can access Internet but the one with VID is 3 can't. That is, visitors in Lobby and staffs in office can access Internet. But ones in Lab can't since security issue. Servers in Lab serve only for trusted staffs or are accessed in secure tunnels.



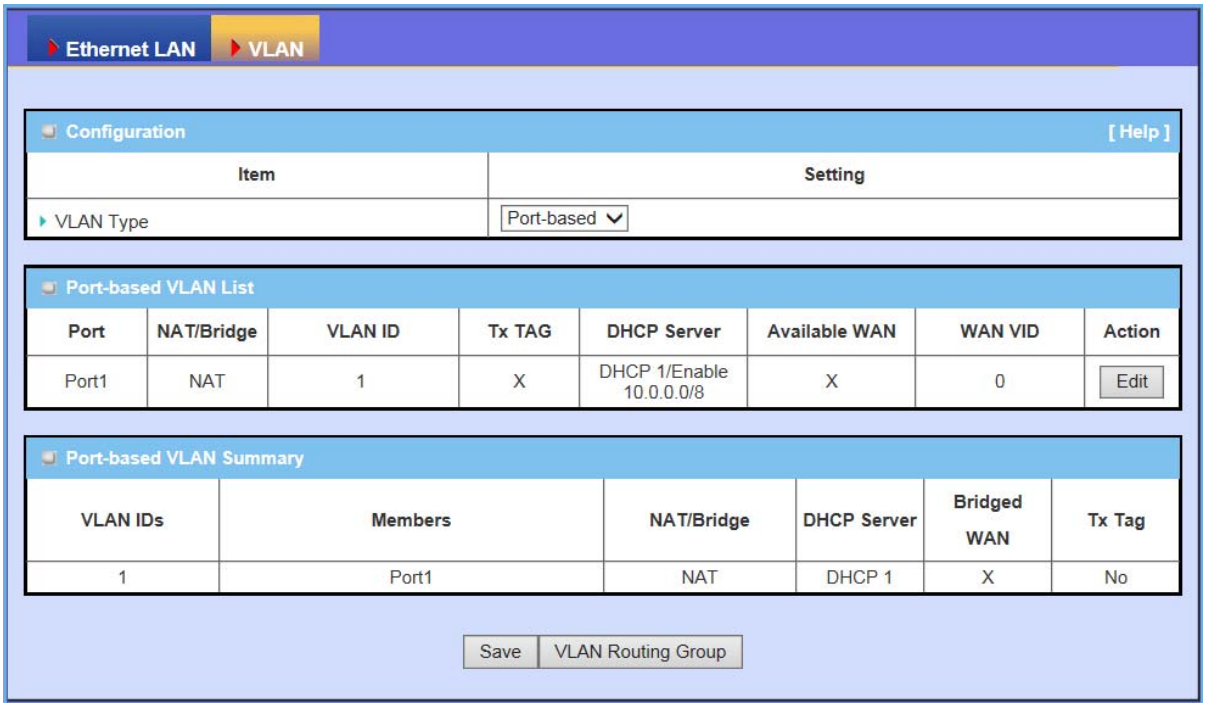
Inter VLAN Group Routing:

In Port-based tagging, administrator can specify member hosts of one VLAN group to be able to communicate with the ones of another VLAN group or not. This is a communication pair, and one VLAN group can join many communication pairs. But communication pair has not the transitive property. That is, A can communicate with B, and B can communicate with C, that doesn't mean A can communicate with C. An example is shown at following diagram. VLAN groups of VID is 1 and 3 can access each other but the ones between VID 3 and VID 4 and between VID 1 and VID 4 can't.



3.1.2.2.2 Port-Based VLAN

Since there is only one physical Ethernet LAN port in the gateway, there is little configuration need to do if you choose the Port-based VLAN. There is only one default VLAN group settings for the Port-based VLAN. All client hosts in the VLAN group will access Internet via the NAT mechanism in the gateway and get their IP addresses from DHCP server 1. But you can configure the VLAN group to be a Bridge type of application by clicking on the "Edit" button, so the gateway can bridges the Intranet to WAN interface.



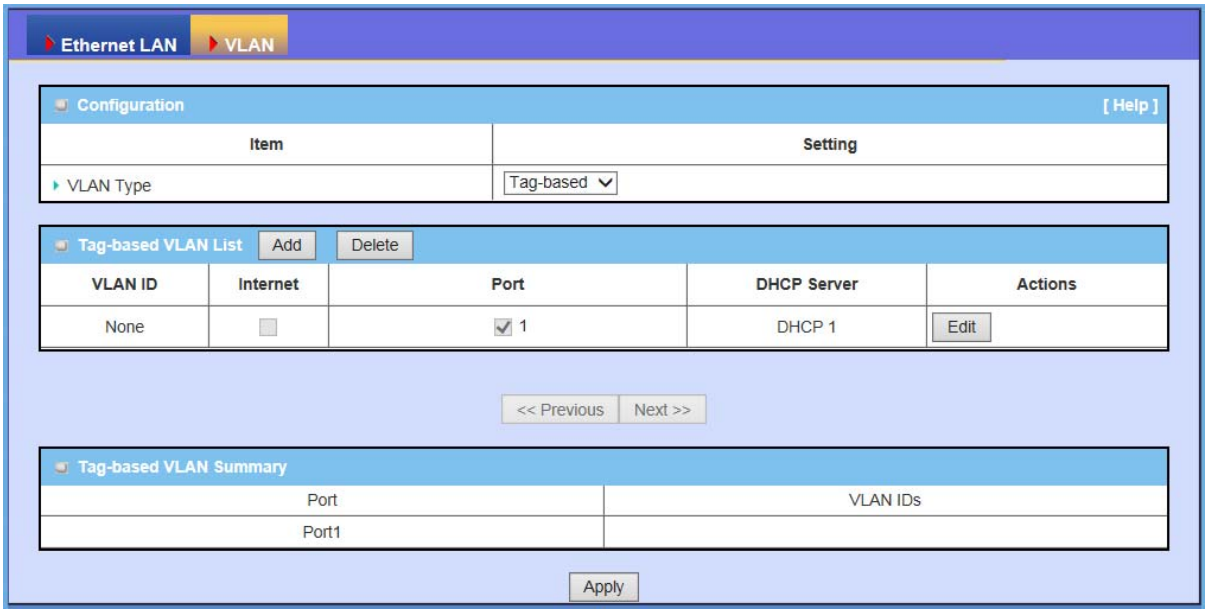
1. **Type**: Select “NAT” or “Bridge” to identify if the packets are directly bridged to the WAN port or processed by NAT mechanism.
2. **LAN VID**: Specify a VLAN identifier for this port. The ports with the same VID are in the same VLAN group.
3. **Tx TAG**: If Intranet packets need a **“VLAN Tag”** with them, please check the checkbox of “Tx TAG”.
4. **DHCP Server**: When "NAT" type, you can specify a DHCP server for the configuring VLAN. Since the device has only one Ethernet port, it provides only 1 DHCP server to serve the DHCP requests from the only one VLAN group.
5. **WAN VID**: The VLAN Tag ID that come from the ISP service. For NAT type VLAN, no WAN VLAN tag is allowed and the value is forced to “0”; For Bridge type VLAN, You have to specify the VLAN Tag value that is provided by your ISP.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.1.2.2.3 Tag-Based VLAN

The second type of VLAN is the tag-based VLAN. VLAN membership in a tagged VLAN is determined by VLAN information within the packet frames that are received on a port. This differs from a port-based VLAN, where the port ID with different VLAN ID determine VLAN membership.

When the device receives a frame with a VLAN tag, referred to as a tagged frame, the device forwards the frame only to those ports that share the same VID.



By default, all the LAN ports belong to one VLAN group, and this VLAN ID is forced to denoted as “None”. It is a special tag-based VLAN for device to operated, there is no tag required to be carried in the packets for this default VLAN group.

You can edit the default VLAN group by clicking on the "Edit" button. You also can add one new VLAN group by clicking on the "Add" command.

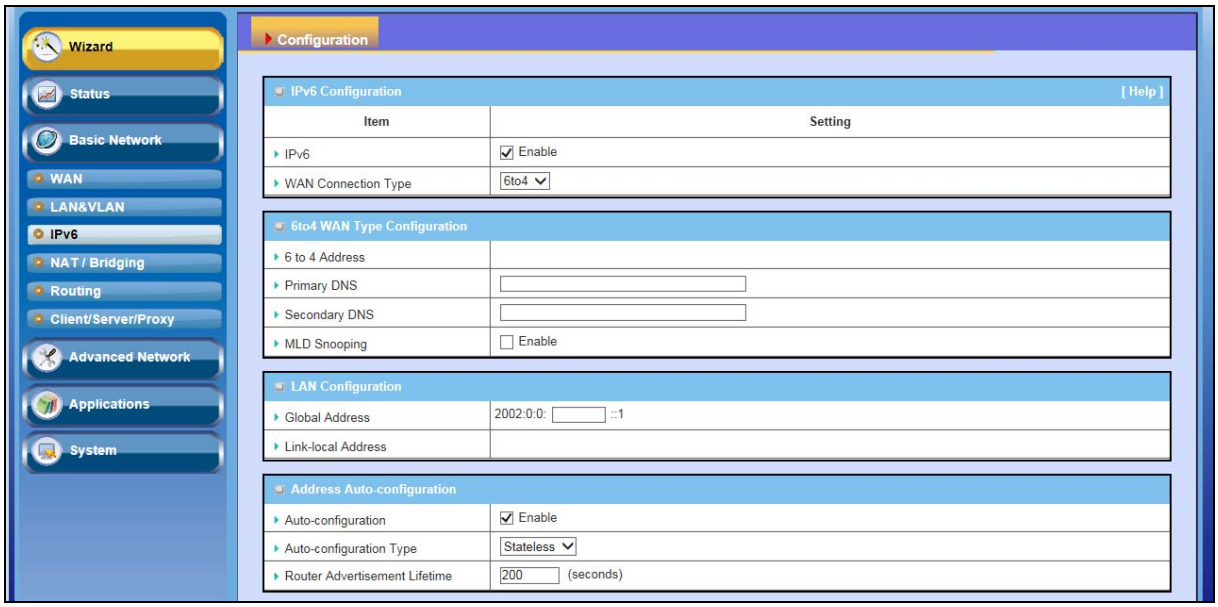
1. **VLAN ID**: Specify a VLAN tag for this VLAN group. The packets with the same VID will be transferred between the client hosts of same VLAN group.
2. **Internet**: Specify whether this VLAN group can access Internet or not. If it is checked, all the packet will be un-tagged before it is forward to Internet, and all the packets from Internet will be tagged with the VLAN ID before it is forward to the destination belongs to this configuring VLAN group in the Intranet.
3. **Port**: Specify what Ethernet LAN ports can deliver the packets that carry specific VLAN tag for the VLAN group. You just have to check the boxes for dedicated ports for the group. But the device has only one Ethernet LAN port.
4. **DHCP Server**: Specify a DHCP server for the configuring VLAN. This device provides 1 DHCP server to serve the DHCP requests from different VLANs.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

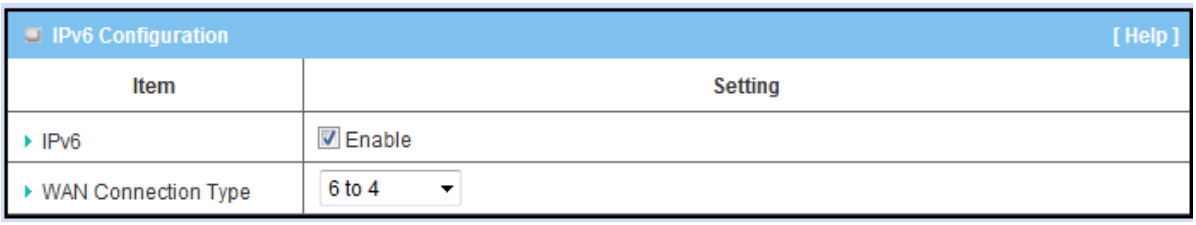
3.1.3 IPv6 Setup

The growth of the Internet has created a need for more addresses than are possible with IPv4. **IPv6** (**Internet Protocol version 6**) is a version of the Internet Protocol (IP)

intended to succeed IPv4, which is the protocol currently used to direct almost all Internet traffic. IPv6 also implements additional features not present in IPv4. It simplifies aspects of address assignment (stateless address auto-configuration), network renumbering and router announcements when changing Internet connectivity providers. This gateway supports two types of IPv6 connection (6to4 / 6in4). **Please ask your ISP of what type of IPv6 is supported before you proceed with IPv6 setup.**

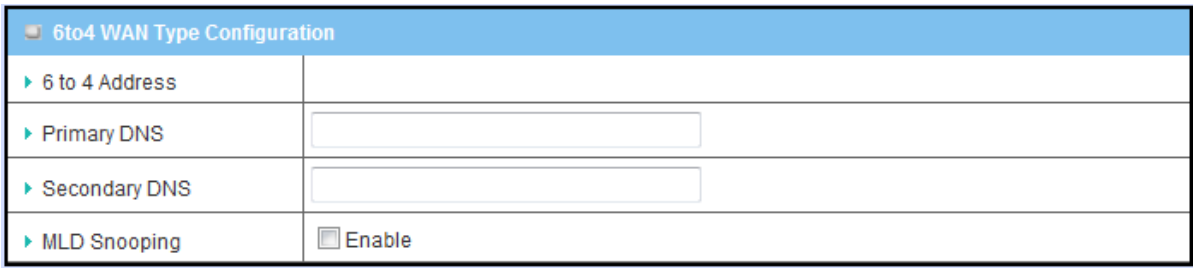


3.1.3.1 6 to 4



When “6 to 4” is selected for the WAN Connection Type, you need to do the following settings:

6to4 WAN Type Configuration

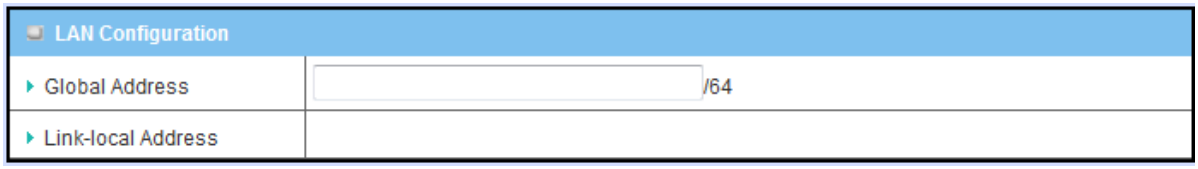


1. **6 to 4 Address**: You may obtain IPv6 DNS automatically or set DNS address

manually for Primary DNS address and secondary DNS address.

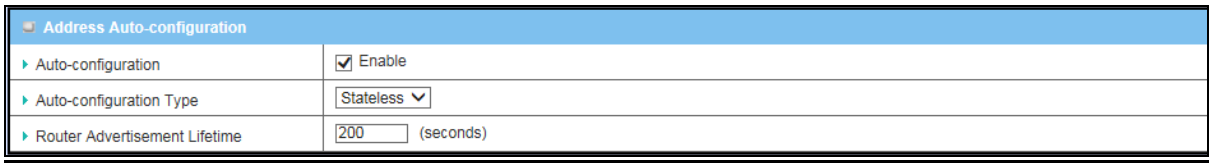
2. **Primary / Secondary DNS:** Please enter IPv6 primary DNS address and secondary DNS address.
3. **MLD Snooping:** MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets. If necessary in your environment, please enable this feature.

LAN Configuration



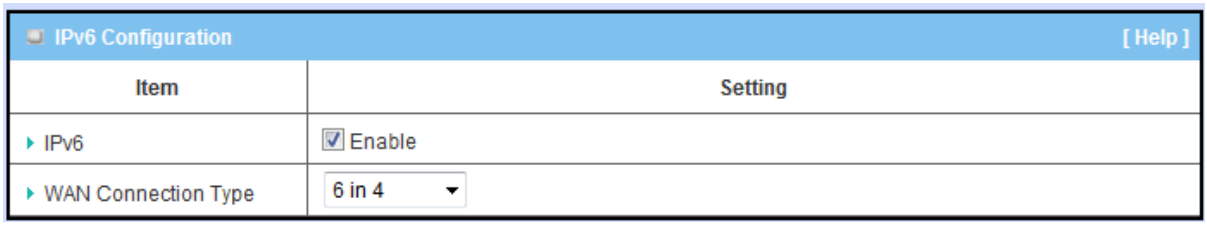
1. **Global Address:** Please enter IPv6 global address for LAN interface.
2. **Link-local Address:** To show the IPv6 Link-local address of LAN interface.

Address Auto-configuration



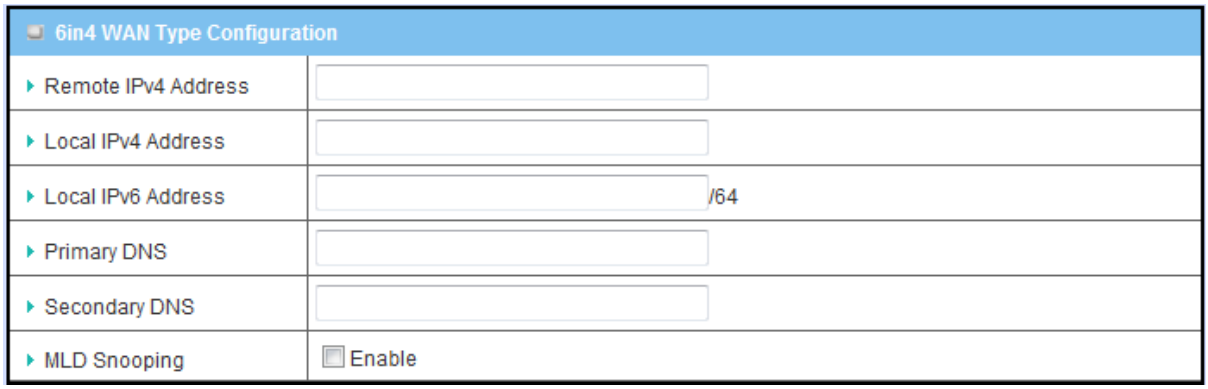
1. **Auto-configuration:** Disable or enable this auto configuration setting.
2. **Auto-configuration type:** You may set stateless or stateful (Dynamic IPv6).
3. **Router Advertisement Lifetime:** You can set the time for the period that the router send (broadcast) its router advertisement. Each router periodically multicasts a Router Advertisement from each of its multicast interfaces, announcing the IP address of that interface. Hosts discover the addresses of their neighboring routers simply by listening for advertisements. When a host attached to a multicast link starts up, it may multicast a Router Solicitation to ask for immediate advertisements, rather than waiting for the next periodic ones to arrive; if and only if no advertisements are forthcoming, the host may retransmit the solicitation a small number of times, but then must desist from sending any more solicitations. Any routers that subsequently start up, or that were not discovered because of packet loss or temporary link partitioning, are eventually discovered by reception of their periodic (unsolicited) advertisements.

3.1.3.2 6 in 4



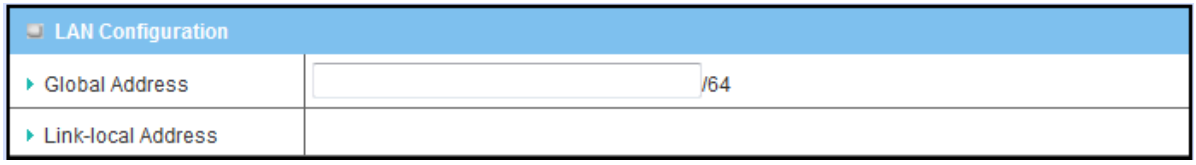
When “6 in 4” is selected for the WAN Connection Type, you need to do the following settings:

6in4 WAN Type Configuration



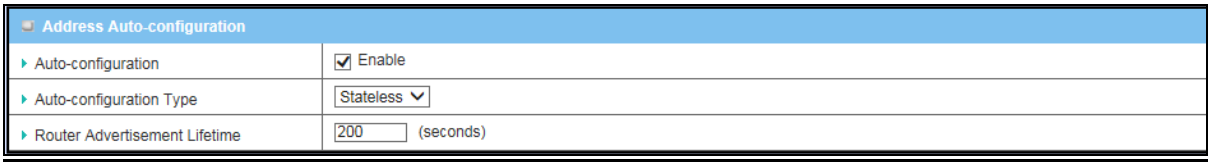
1. **Remote / Local IPv4 and IPv6 Address**: you may add remote / local IPv4 address and local IPv6 address, then set DNS address manually for Primary DNS address and secondary DNS address.
2. **DNS:** Please enter IPv6 primary DNS address and secondary DNS address.
3. **MLD Snooping:** MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets. If necessary in your environment, please enable this feature.

LAN Configuration



1. **Global Address:** Please enter IPv6 global address for LAN interface.
2. **Link-local Address:** To show the IPv6 Link-local address of LAN interface.

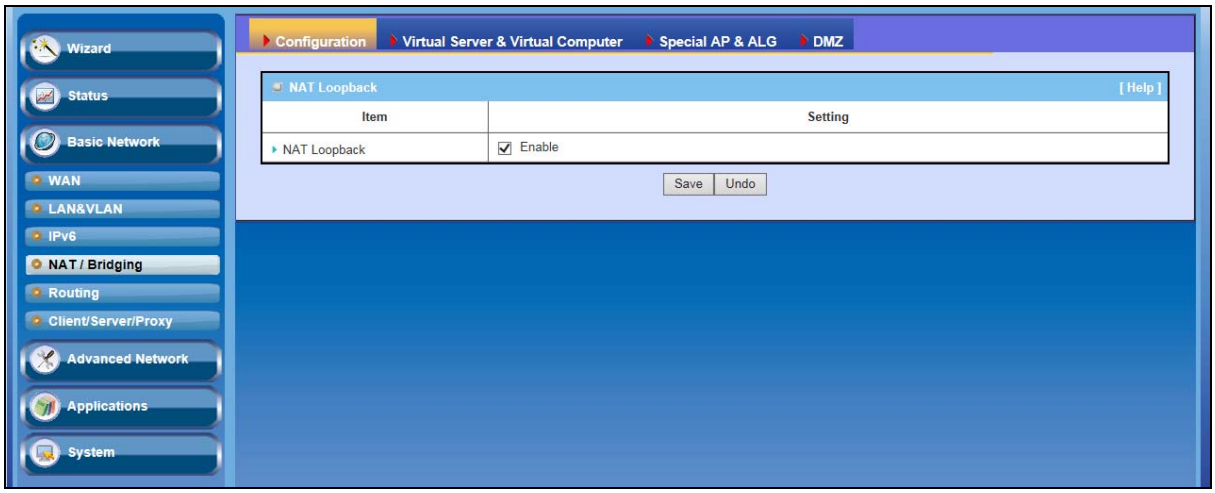
Address Auto-configuration



1. **Auto-configuration:** Disable or enable this auto configuration setting.
2. **Auto-configuration Type:** You may set stateless or stateful (Dynamic IPv6).
3. **Router Advertisement Lifetime:** You can set the time for the period that the router send (broadcast) its router advertisement. Each router periodically multicasts a Router Advertisement from each of its multicast interfaces, announcing the IP address of that interface. Hosts discover the addresses of their neighboring routers simply by listening for advertisements. When a host attached to a multicast link starts up, it may multicast a Router Solicitation to ask for immediate advertisements, rather than waiting for the next periodic ones to arrive; if and only if no advertisements are forthcoming, the host may retransmit the solicitation a small number of times, but then must desist from sending any more solicitations. Any routers that subsequently start up, or that were not discovered because of packet loss or temporary link partitioning, are eventually discovered by reception of their periodic (unsolicited) advertisements.

3.1.4 NAT / Bridging

This part includes NAT related settings, such as NAT Loopback, Virtual Server, Virtual Computer, Special AP, ALG and DMZ.



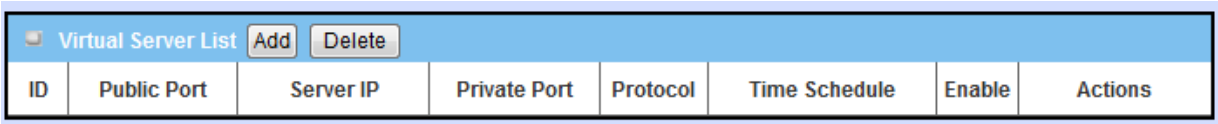
3.1.4.1 Configuration

1. **NAT Loopback:** Allow you to access the WAN IP address from inside your local network. This is useful when you run a server inside your network. For an

example, if you set a mail server at LAN side, your local devices can access this mail server through gateway's WAN IP address. You don't need to change IP address of mail server no matter you are at local side or go out. This is useful when you run a server inside your network.

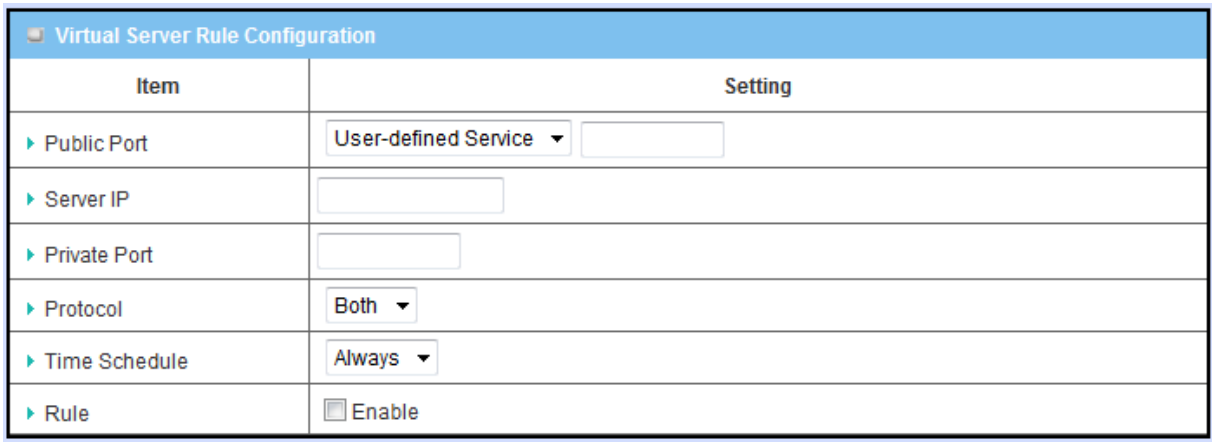
3.1.4.2 Virtual Server & Virtual Computer

3.1.4.2.1 Virtual Server



This gateway's NAT firewall filters out unrecognized packets to protect your Intranet, so all hosts behind this device are invisible to the outside world. If you wish, you can make some of them accessible by enabling the Virtual Server Mapping. Press "Add" button to add new rule for Virtual Server.

A virtual server is defined as a **Public Port**, and all requests to this port will be redirected to the computer specified by the **Server IP.** Virtual Server can work with **Scheduling Rules**, and give user more flexibility on Access control. For the details, please refer to **[System]-[Scheduling]**.



For example, if you have an **FTP server (Service port 21) at 10.0.75.1**, a **Web server1 (Service port 80) at 10.0.75.2,** a **Web server2 (Service Port 8080 and Private port 80) at 10.0.75.3,** and a **VPN server at 10.0.75.6,** then you need to specify the following virtual server mapping table

Public Port	Server IP	Private Port	Protocol	Rule
21	10.0.75.1		TCP	Enable
80	10.0.75.2		TCP	Enable
8080	10.0.75.3	80	TCP	Enable
1723	10.0.75.6		Both	Enable

3.1.4.2.2 Virtual Computer

Virtual Computer enables you to use the original NAT feature, and allows you to setup the one-to-one mapping of multiple global IP address and local IP address. Press “Add” button to add new rule for Virtual Computer.

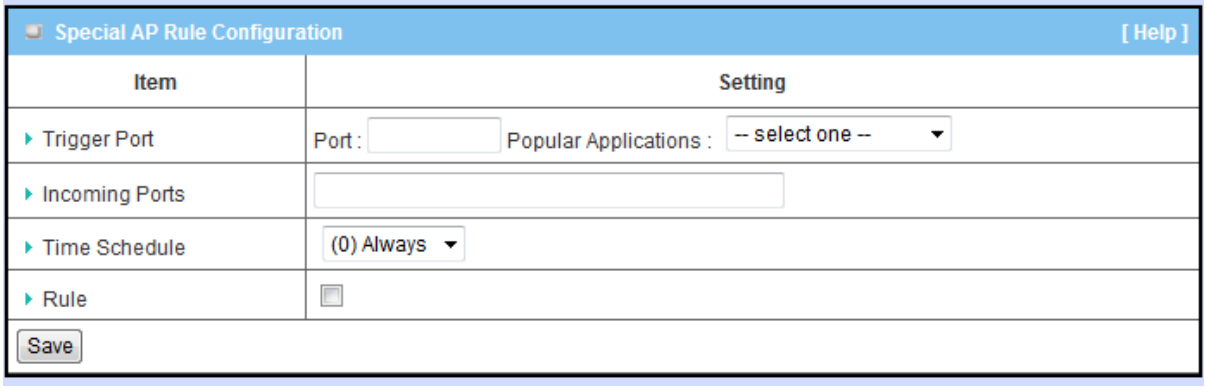
1. **Global IP**: Enter the global IP address assigned by your ISP.
2. **Local IP**: Enter the local IP address of your LAN PC corresponding to the global IP address.
3. **Enable**: Check this item to enable the Virtual Computer feature.

3.1.4.3 Special AP & ALG

NAT feature can protect Intranet from outside attacks, but sometimes also blocks some applications, such as SIP VoIP. In this situation, the NAT gateway needs to do special process (ALG) for each application. This gateway can handle SIP ALG, so you need to enable this option if you want to use SIP applications at LAN side of this gateway.

Some applications require multiple connections, like Internet games, Video conferencing, Internet telephony, etc. Because of the firewall function, these applications cannot work with a pure NAT router. **The Special Applications** feature allows some of these applications to work with this product. If the mechanism of Special Applications fails to make an application work, try setting your computer as the DMZ host instead.

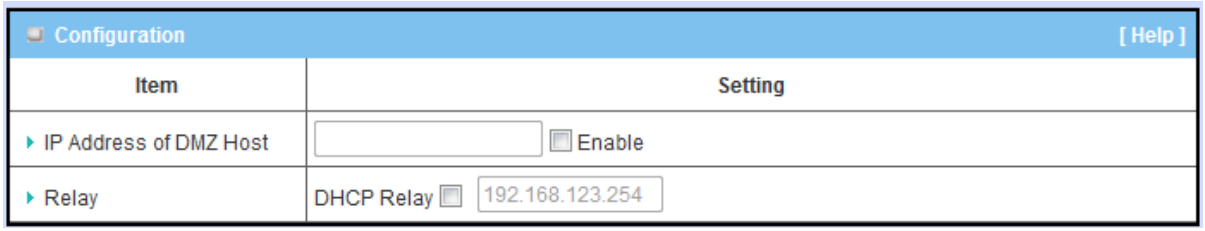
Press “Add” button to add new rule for Special AP.



This device provides some predefined settings. Select your application item, and all related settings will be filled up automatically.

1. **Trigger Port:** The outbound port number issued by the application.
2. **Incoming Ports**: When the trigger packet is detected, the inbound packets sent to the specified port numbers are allowed to pass through the firewall.
3. **Time Schedule**: Each special AP setting can be turned off according to the schedule rule you specified. By default, it is always turned on when the rule is enabled.
4. **Rule**: Check this item to enable the Special AP rule.

3.1.4.4 DMZ



DMZ (DeMilitarized Zone) Host is a host without the protection of firewall. It allows a computer to be exposed to unrestricted 2-way communication for Internet games, Video conferencing, Internet telephony and other special applications. Otherwise, if specific application is blocked by NAT mechanism, you can indicate that LAN computer as a DMZ host to solve this problem.

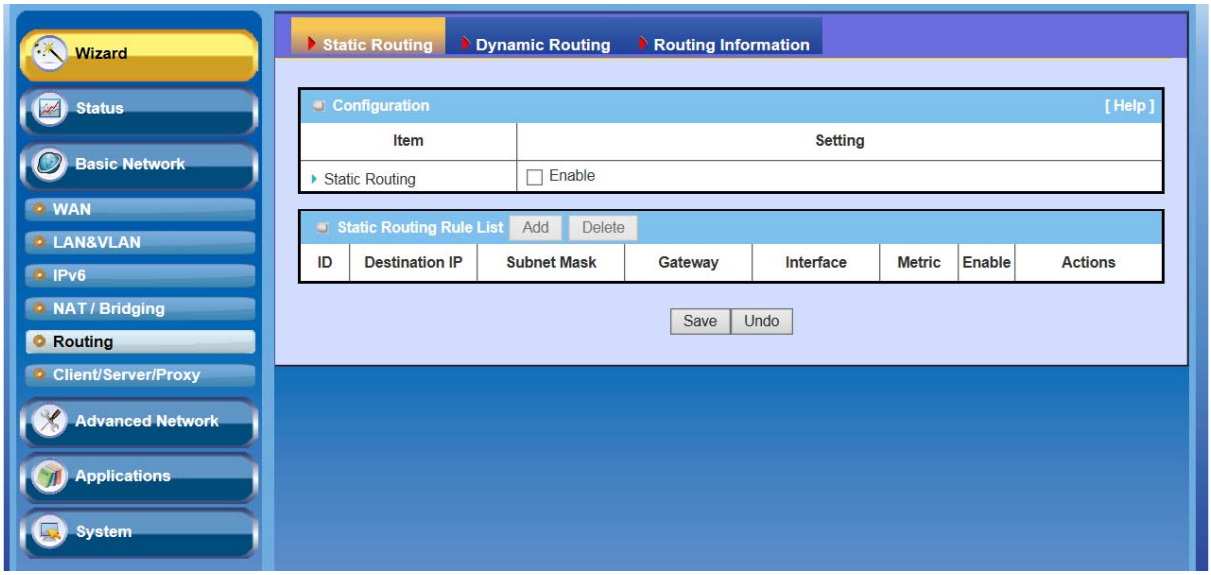
1. **IP Address of DMZ Host:** Enter IP address of Server or Host.
2. **DHCP Relay**: DHCP Relay Agent component relays DHCP messages between DHCP clients and DHCP servers on different IP networks. Because DHCP is a broadcast-based protocol, by default its packets do not pass through routers. If

you need this feature in the environment, please enable it.

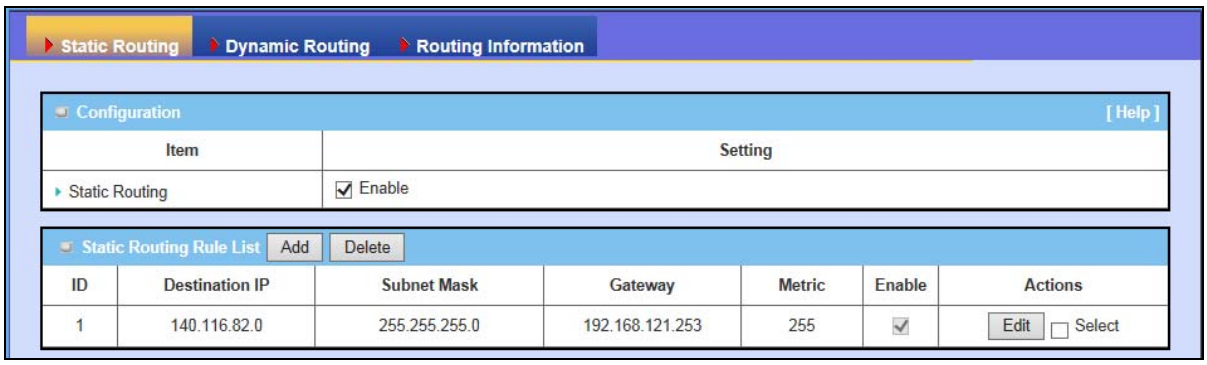
NOTE: This feature should be used only when needed.

3.1.5 Routing Setup

If you have more than one router and subnet, you will need to enable routing function to allow packets to find proper routing path and allow different subnets to communicate with each other.

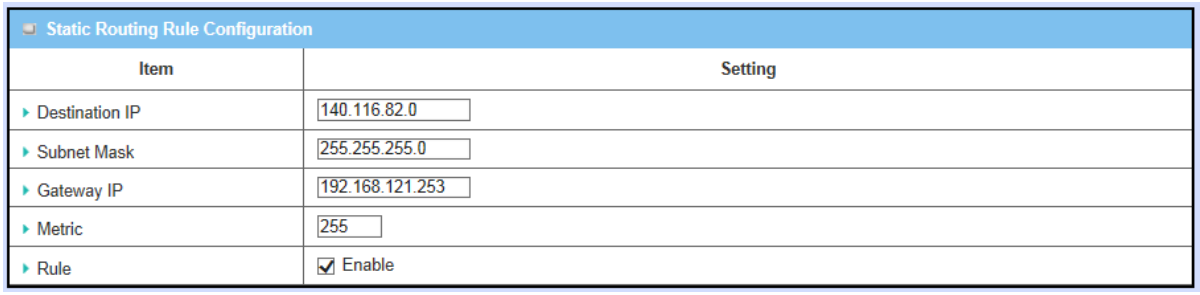


3.1.5.1 Static Routing



For static routing, you can specify up to 32 routing rules. The routing rules allow you to determine which physical interface addresses are utilized for outgoing IP data grams. You can enter the **destination IP address**, **Subnet Mask**, **Gateway**, and **Metric** for each routing rule, and then enable or disable the rule by checking or un-checking the Enable checkbox.

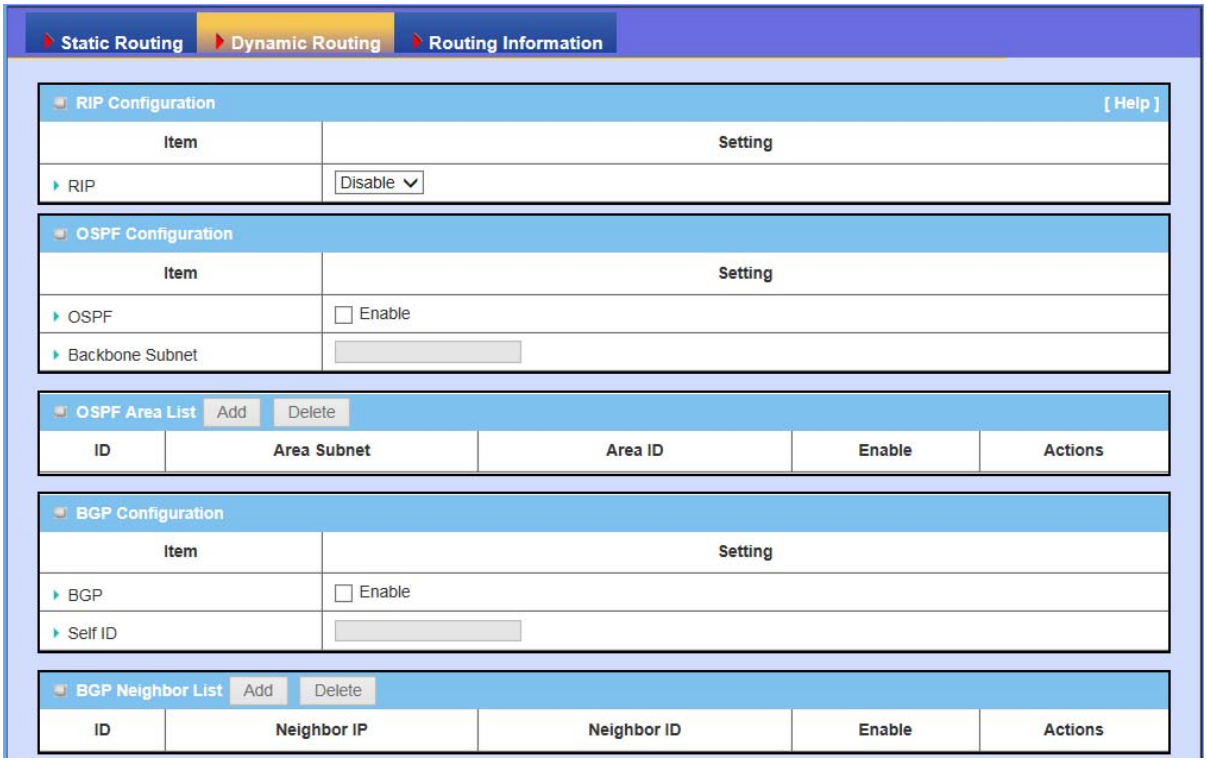
Please click Add or Edit button to configure a static routing rule:



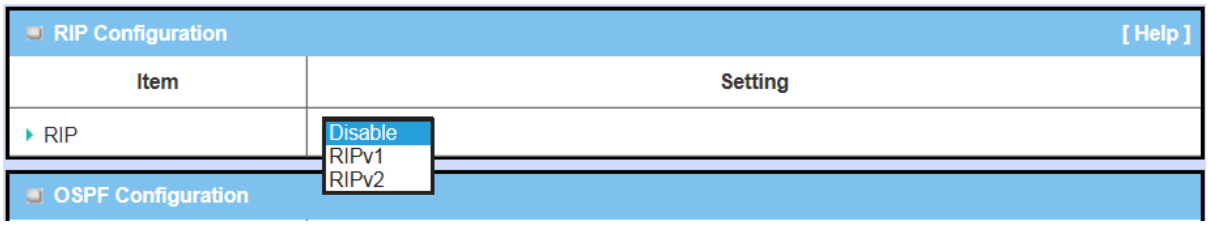
1. **Destination IP:** Enter the subnet network of routed destination.
2. **Subnet Mask:** Input your subnet mask. Subnet mask defines the range of IP address in destination network.
3. **Gateway:** The IP address of gateway that you want to route for this destination subnet network. The assigned gateway is required to be in the same subnet of LAN side or WAN side.
4. **Metric:** The router uses the value to determine the best possible route. It will go in the direction of the gateway with the lowest metric.
5. **Rule:** Check the Enable box to enable this static routing rule.

3.1.5.2 Dynamic Routing

The feature of static route is for you to maintain routing table manually. In addition, this gateway also supports dynamic routing protocol, such as RIPv1/RIPv2, OSPF, BGP for you to establish routing table automatically. The feature of dynamic routing will be very useful when there are lots of subnets in your network. Generally speaking, RIP is suitable for small network. OSPF is more suitable for medium network. BGP is more used for big network infrastructure.



3.1.5.2.1 RIP



1. **RIP**: Routing Information Protocol (RIP) will exchange information about destinations for computing routes throughout the network. Please select RIPv2 only if you have different subnets in your network. Otherwise, please select RIPv1 if you need this protocol.

3.1.5.2.2 OSPF

OSPF is an interior gateway protocol that routes Internet Protocol (IP) packets solely within a single routing domain (autonomous system). It gathers link state information from available routers and constructs a topology map of the network. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP packets.

OSPF Configuration

Item	Setting
OSPF	Enable
Backbone Subnet	192.168.121.0/24

OSPF Area List Add Delete

ID	Area Subnet	Area ID	Enable	Actions
1	192.168.122.0/24	192.168.122.1	☑	Edit Select
2	192.168.123.0/24	192.168.123.1	☑	Edit Select
3	192.168.124.0/24	192.168.124.1	☑	Edit Select

You can enable the OSPF routing function by click on the “Enable” button for OSPF item. There are 8 area subnets can be defined in the OSPF network and enable them individually. When you finished setting, click on **“Save”** to store your settings. Above settings are just for examples.

3.1.5.2.3 BGP

Border Gateway Protocol (BGP) is the protocol backing the core routing decisions on the Internet. It maintains a table of IP networks or 'prefixes' which designate network reach-ability among autonomous systems (AS). It is described as a path vector protocol. BGP does not use traditional Interior Gateway Protocol (IGP) metrics, but makes routing decisions based on path, network policies and/or rule-sets. For this reason, it is more appropriately termed a reach-ability protocol rather than routing protocol.

BGP Configuration

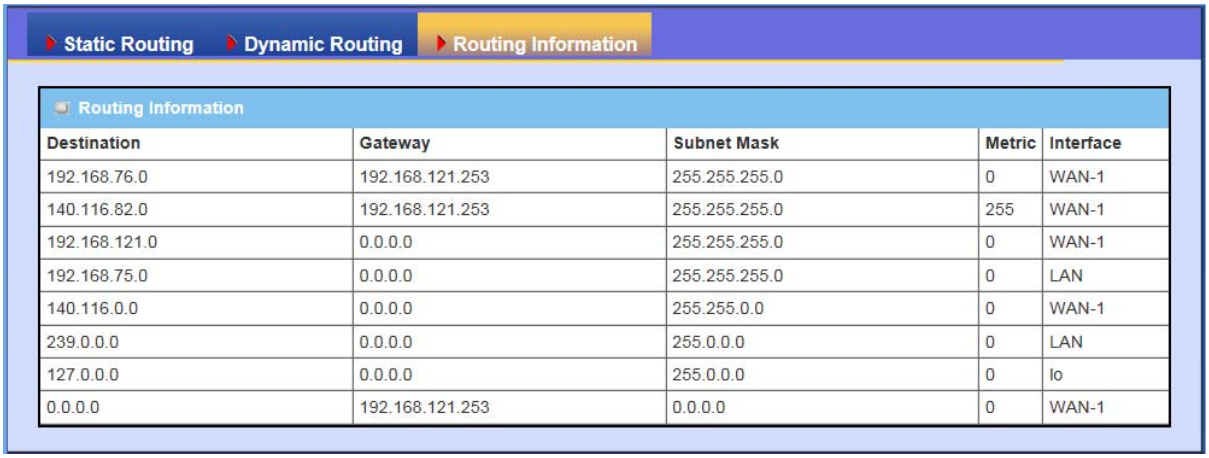
Item	Setting
BGP	Enable
Self ID	100

BGP Neighbor List Add Delete

ID	Neighbor IP	Neighbor ID	Enable	Actions
1	10.101.0.1	101	☑	Edit Select
2	10.102.0.1	102	☑	Edit Select
3	10.103.0.1	103	☑	Edit Select
4	10.104.0.1	104	☑	Edit Select

You can enable the BGP routing function by click on the “Setting” button and fill in the corresponding setting for your BGP routing configuration. When you finished setting, click on **“Save”** to store your settings or click **“Undo”** to give up the changes. Above settings are just for examples.

3.1.5.3 Routing Information



Destination	Gateway	Subnet Mask	Metric	Interface
192.168.76.0	192.168.121.253	255.255.255.0	0	WAN-1
140.116.82.0	192.168.121.253	255.255.255.0	255	WAN-1
192.168.121.0	0.0.0.0	255.255.255.0	0	WAN-1
192.168.75.0	0.0.0.0	255.255.255.0	0	LAN
140.116.0.0	0.0.0.0	255.255.0.0	0	WAN-1
239.0.0.0	0.0.0.0	255.0.0.0	0	LAN
127.0.0.0	0.0.0.0	255.0.0.0	0	lo
0.0.0.0	192.168.121.253	0.0.0.0	0	WAN-1

A routing table, or routing information base (RIB), is a data table stored in a router or a networked computer that lists the routes to particular network destinations, and in some cases, metrics (distances) associated with those routes. The routing table contains information about the topology of the network immediately around it.

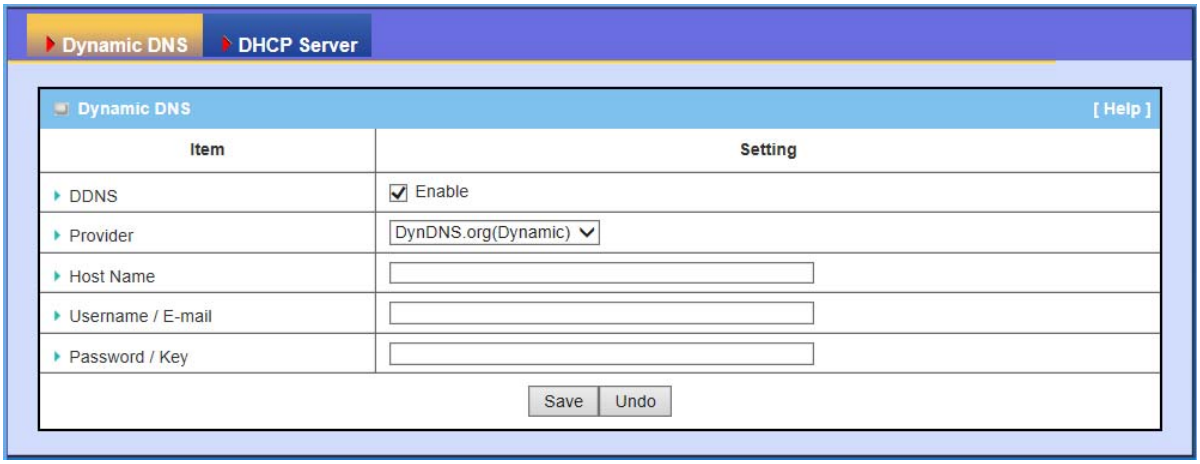
This page displays the routing table maintained by this device. It is generated according to your network configuration, above diagram is just an example.

3.1.6 Client/Server/Proxy

3.1.6.1 Dynamic DNS

How does user access your server if your WAN IP address changes all the time? One way is to register a new domain name, and maintain your own DNS server. Another simpler way is to apply a domain name to 3-party DDNS service provider. It can be free or charged.

To host your server on a changing IP address, you have to use dynamic domain name service (DDNS). Therefore, anyone wishing to reach your host only needs to know the name of it. Dynamic DNS will map the name of your host to your current IP address, which changes each time you connect your Internet service provider. This device supports most popular 3-party DDNS service provider, including TZO.com, No-IP.com, DynDNS.org(Dynamic), DynDNS.org(Custom), and DHS.org. Before you enable **Dynamic DNS**, you need to register an account on one of these Dynamic DNS servers that we list in **Provider** field.



1. **DDNS:** Check the Enable box if you would like to activate this function.
2. **Provider:** The DDNS provider supports service for you to bind your IP (even private IP) with a certain Domain name. You could choose your favorite provider. There are following options:

3. **Host Name:** Register a domain name to the DDNS provider. The fully domain name is concatenated with hostname (you specify) and a suffix(DDNS provider specifies).
4. **Username/E-mail:** Input username or E-mail based on the DDNS provider you registered.
5. **Password/Key:** Input password or key based on the DDNS provider you select.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

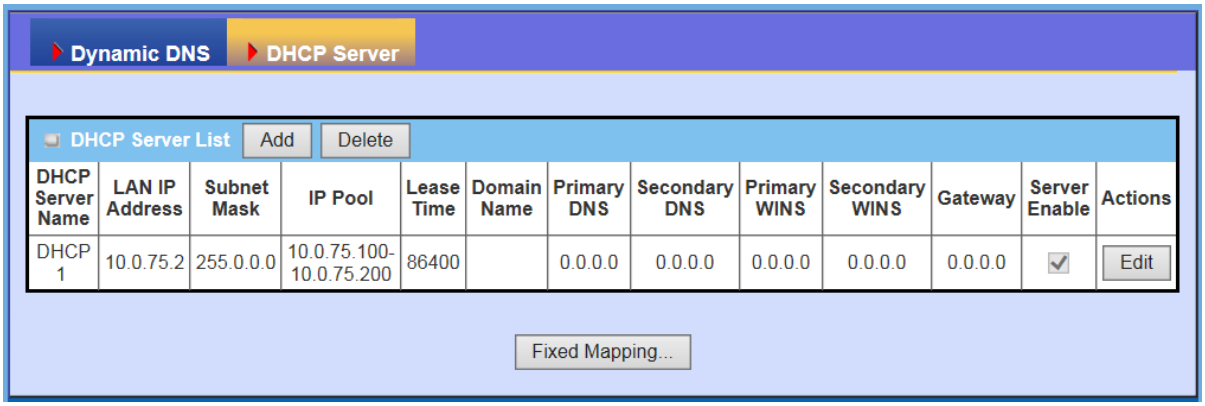
3.1.6.2 DHCP Server

3.1.6.2.1 DHCP Server List

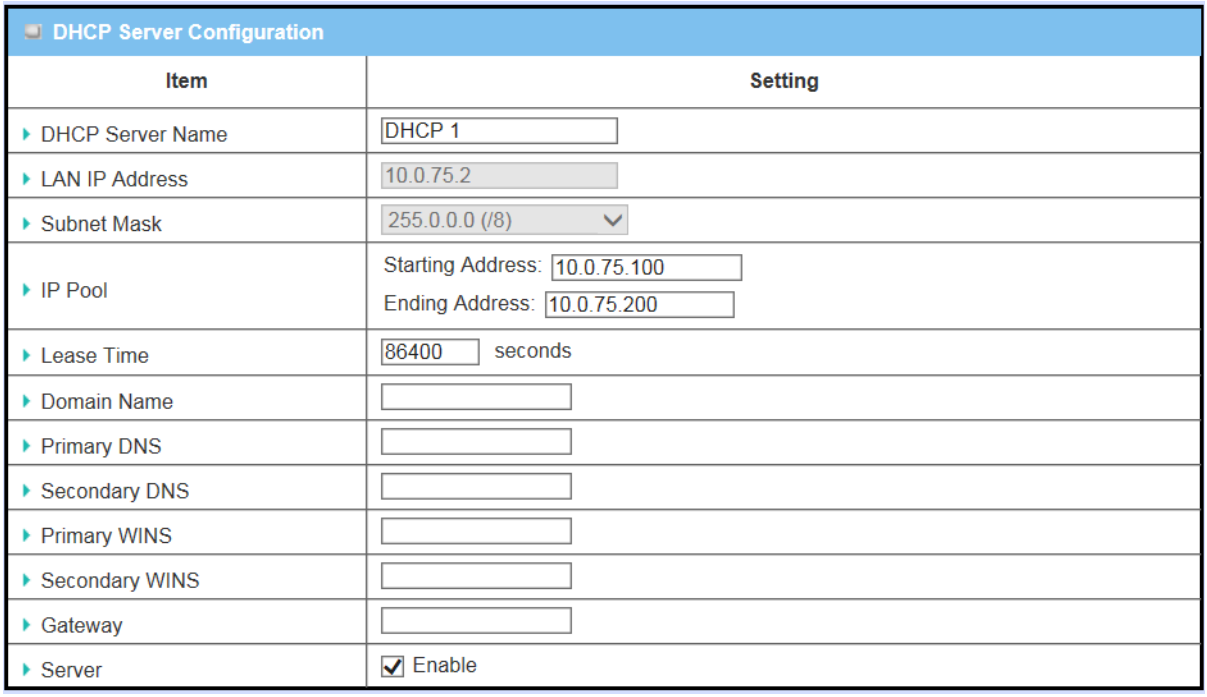
The gateway supports only 1 DHCP server to serve the DHCP requests from different client hosts. And it is the default one whose LAN IP Address is the same one of gateway LAN interface, Subnet Mask is “255.255.255.0”, and IP Pool ranges from .100 to .200 as shown at following DHCP Server List. You can edit the DHCP server configuration by clicking on the “Edit” button at the end of DHCP server information.

There are one additional button can be used to configure the fixed mapping between

MAC address and IP address of local client hosts as following diagram.

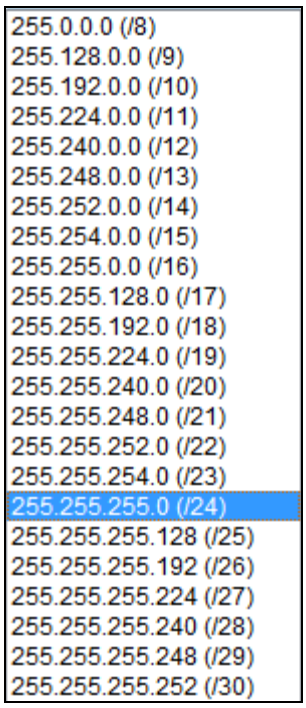


3.1.6.2.2 DHCP Server Configuration



1. **DHCP Server:** Choose DHCP Server to **Enable**. If you enable the DHCP Server function, this gateway will assign IP address to LAN computers or devices through DHCP protocol. This device provides only 1 DHCP server to serve the DHCP requests from different client hosts.
2. **LAN IP Address**: Specify the local IP address of the enabled DHCP Server. It's the LAN IP address of this gateway for DHCP-1 server. Normally, this IP address will be also the default gateway of local computers and devices.
3. **Subnet Mask:** Select the subnet mask for the specific DHCP server. Subnet Mask defines how many clients are allowed in one network or subnet. The default subnet mask is 255.255.255.0/24, and it means maximum 254 IP addresses are allowed in this subnet. However, one of them is occupied by LAN IP address of

this gateway, so there are maximum 253 clients allowed in LAN network. Hereafter are the available options for subnet mask.

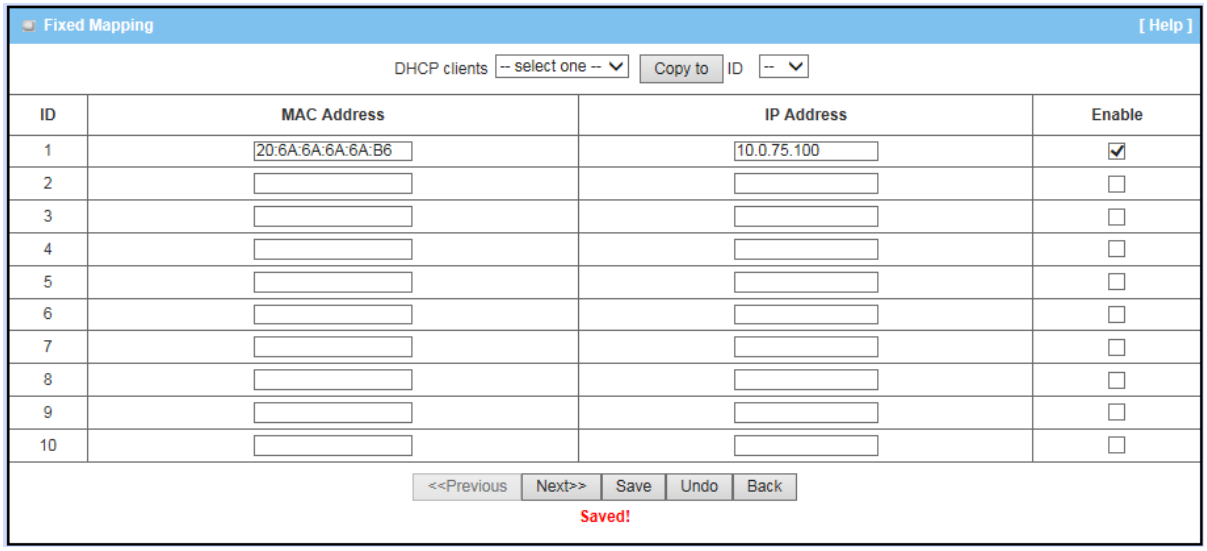


4. **IP Pool Starting / Ending Address:** Whenever there is a request, the DHCP server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting / ending address of the IP address pool. Please note the number of IP address in this IP pool must less than the maximum number of subnet network that according to the subnet mask you set.
5. **Lease Time:** DHCP lease time to the DHCP client.
6. **Domain Name:** Optional, this information will be passed to the clients.
7. **Primary DNS/Secondary DNS:** Optional. This feature allows you to assign DNS Servers.
8. **Primary WINS/Secondary WINS:** Optional. This feature allows you to assign WINS Servers.
9. **Gateway:** Optional. Gateway address would be the IP address of an alternate Gateway. This function enables you to assign another gateway to your local computer when DHCP server offers IP address. For an example, this gateway will assign IP address to local computers, but local computers will go to Internet through another gateway.

3.1.6.2.3 Fixed Mapping

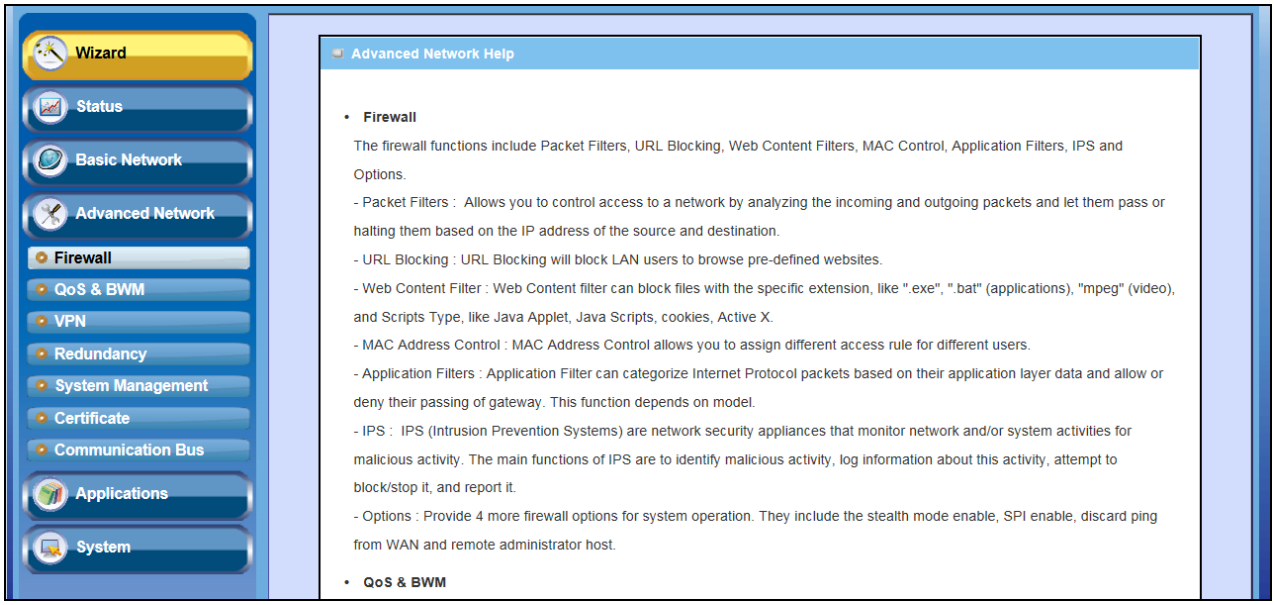
Press **"Fixed Mapping …"** button at the bottom of the DHCP server list page and you can specify a certain IP address for designated local device (MAC address) by manual, so that the DHCP Server will reserve the special IPs for designated devices.

For internal servers, you can use this feature to ensure each of them receives same IP address all the time.



3.2 Advanced Network

This device also supports many advanced network features, such as Firewall, QoS & Bandwidth Management, VPN Security, Redundancy, System Management, Certificate and Communication Bus. You can finish those configurations in this section.

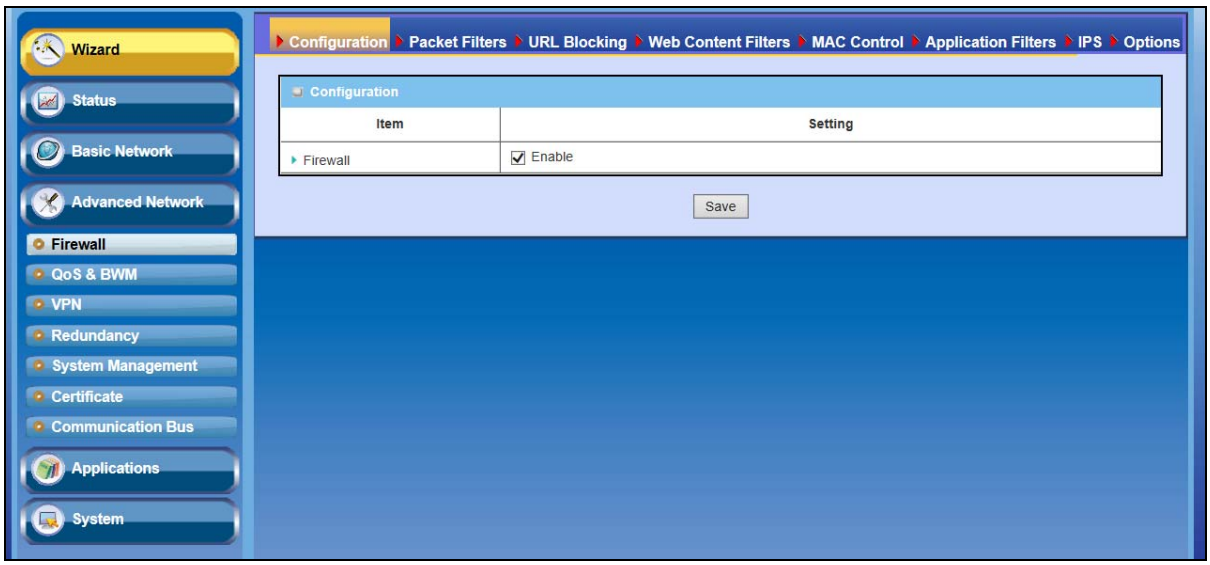

Wizard
Status
Basic Network
Advanced Network
Firewall
QoS & BWM
VPN
Redundancy
System Management
Certificate
Communication Bus
Applications
System
Advanced Network Help
Firewall
The firewall functions include Packet Filters, URL Blocking, Web Content Filters, MAC Control, Application Filters, IPS and Options.
- Packet Filters : Allows you to control access to a network by analyzing the incoming and outgoing packets and let them pass or halting them based on the IP address of the source and destination.
- URL Blocking : URL Blocking will block LAN users to browse pre-defined websites.
- Web Content Filter : Web Content filter can block files with the specific extension, like ".exe", ".bat" (applications), "mpeg" (video), and Scripts Type, like Java Applet, Java Scripts, cookies, Active X.
- MAC Address Control : MAC Address Control allows you to assign different access rule for different users.
- Application Filters : Application Filter can categorize Internet Protocol packets based on their application layer data and allow or deny their passing of gateway. This function depends on model.
- IPS : IPS (Intrusion Prevention Systems) are network security appliances that monitor network and/or system activities for malicious activity. The main functions of IPS are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it.
- Options : Provide 4 more firewall options for system operation. They include the stealth mode enable, SPI enable, discard ping from WAN and remote administrator host.
QoS & BWM

3.2.1 Firewall

The firewall functions include Packet Filters, URL Blocking, Web Content Filters, MAC Control, Application Filters, IPS and some firewall options.

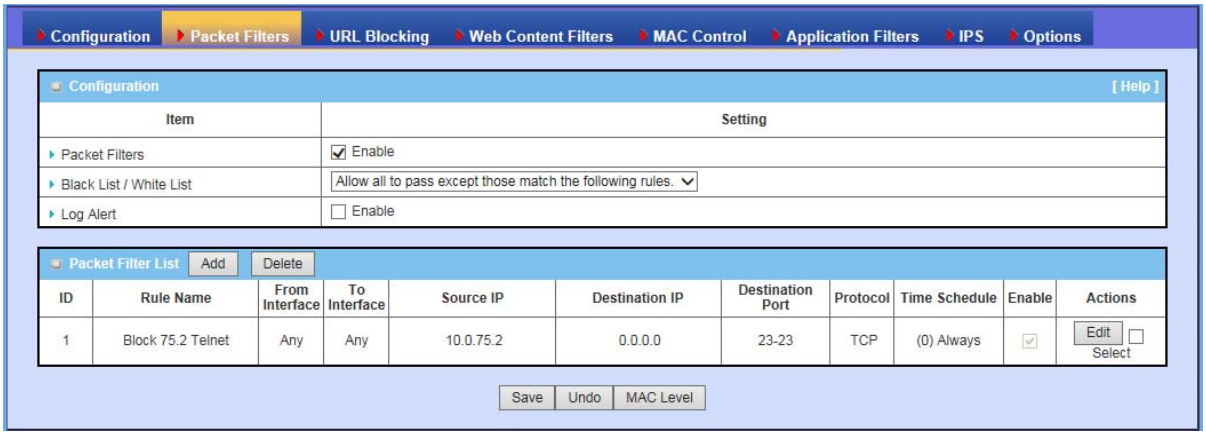
3.2.1.1 Configuration

One Firewall Enable check box lets you activate some firewall functions that you want.



3.2.1.2 Packet Filters

Packet Filters function can let you define both outbound filter and inbound filter rules by specifying the source IP and destination IP in a rule. It enables you to control what packets are allowed or blocked to pass the router. Outbound filters are applied to all outbound packets. However, inbound filters are applied to packets that destined to virtual servers or DMZ host / port only.

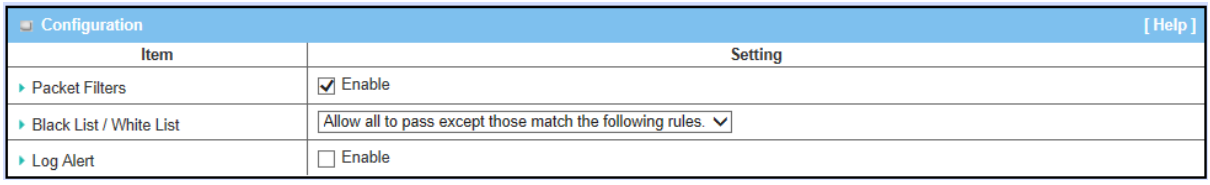


3.2.1.2.1 Configuration

You can enable packet filter function here. And select one of the two filtering policies as follows. The first one is to define the black list. System will block the packets that match the active filter rules. However, the second one is the white list. System will

allow the packets to pass the gateway, which match the active filter rules.

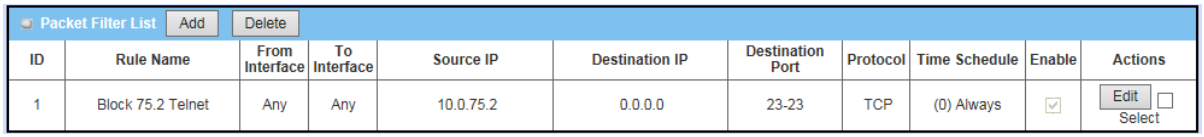
1. Allow all to pass except those match the specified rules. (Black List)
2. Deny all to pass except those match the specified rules. (White List)



Besides, you also can enable the log alerting so that system will record packet blocking events when filter rules are fired. At the right upper corner of screen, one "[Help]" command let you see the on-line help message about Packet Filter function.

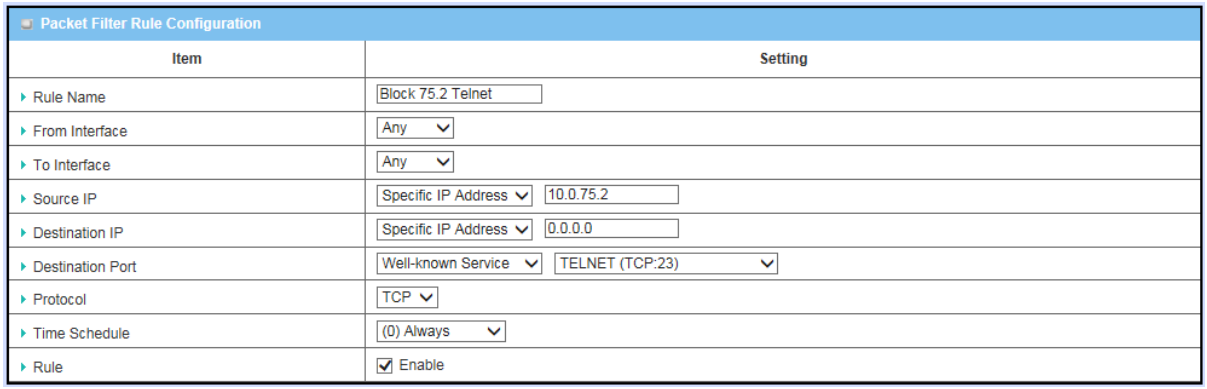
3.2.1.2.2 Packet Filter List

It is a list of all packet filter rules. You can add one new rule by clicking on the "Add" command button. But also you can modify some existed packet filter rules by clicking corresponding "Edit" command buttons at the end of each filter rule in the Packet Filter List. Besides, unnecessary rules can be removed by checking the "Select" box for those rules and then clicking on the "Delete" command button at the Packet Filter List caption.

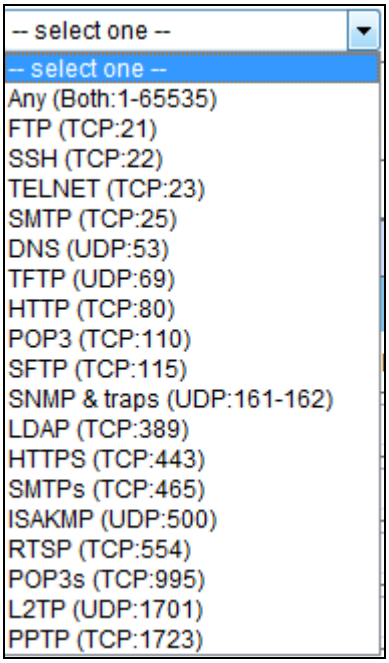


3.2.1.2.3 Packet Filter Rule Configuration

It supports the adding of one new rule or the editing of one existed rule. There are some parameters need to be specified in one packet filter rule. They are Rule Name, From Interface, To Interface, Source IP, Destination IP, Destination Port, Protocol, Time Schedule and finally, the rule enable.



1. **Rule Name:** The name of packet filter rule.
2. **From Interface:** Any interface or someone LAN interface or someone WAN interface.
3. **To Interface:** Any interface or someone LAN interface or someone WAN interface.
4. **Source IP:** Specify the Source IP address of packets that want to be filtered out in the packet filter rule. You can define a single IP address (4.3.2.1) or a range of IP addresses (4.3.2.20~30). A “0.0.0.0” implies all IP addresses.
5. **Destination IP:** Specify the Destination IP address of packets that want to be filtered out in the packet filter rule. You can define a single IP address (4.3.2.1) or a range of IP addresses (4.3.2.20~30). A “0.0.0.0” implies all IP addresses.
6. **Destination Port:** Choose “User-defined Service” to let you specify manually the destination service port of packets that want to be filtered out in the packet filter rule. You can define a single port (80) or a range of ports (1000-1999). A “0” implies all ports are used. You also can choose one well-known service instead so that the chosen service will provide its destination port and protocol number for the rule. The supported well-known services include:

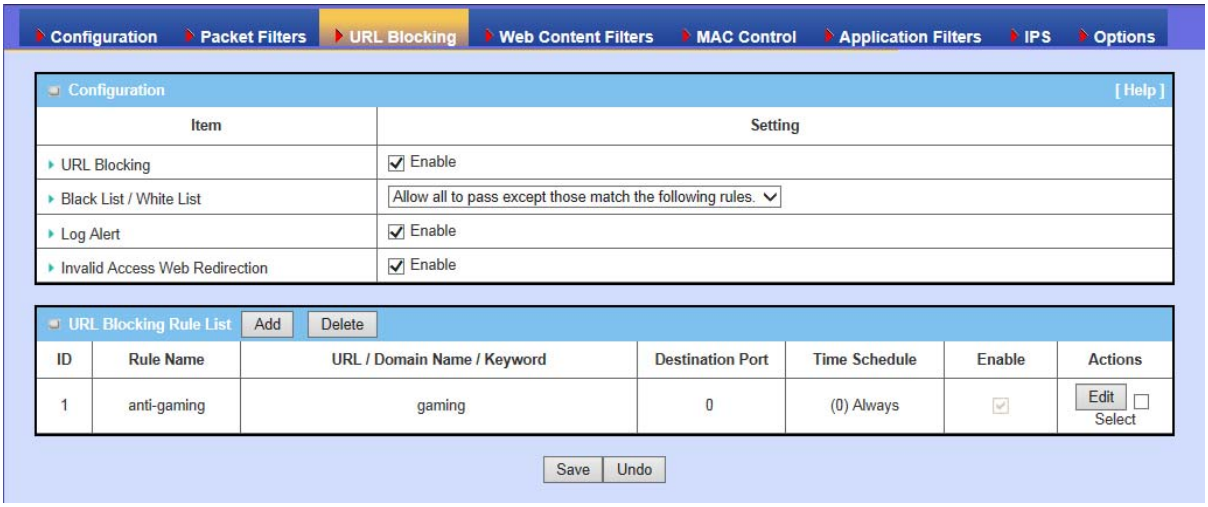


7. **Protocol:** Specify which packet protocol is to be filtered. It can be TCP, UDP, or Both.
8. **Time Schedule:** The rule can be turn on according to the schedule rule you specified, and give user more flexibility on access control. By default, it is always turned on when the rule is enabled. For more details, please refer to the **System** -> **Scheduling** menu.
9. **Rule Enable:** Check the enable box if you want to activate the rule. Each rule can be enabled or disabled individually.

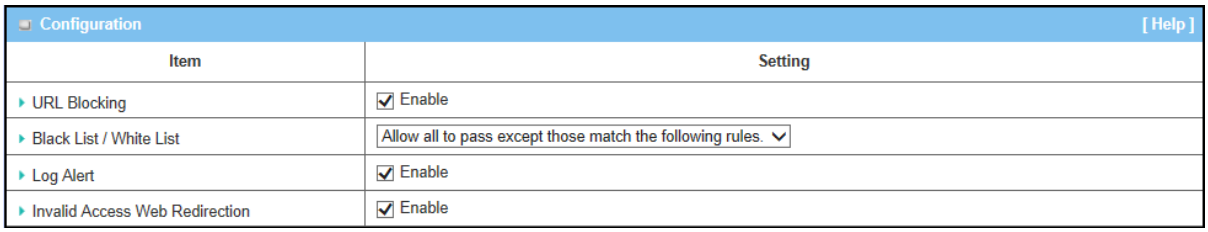
Afterwards, click on **"Save"** to store your settings or click **"Undo"** to give up the changes.

3.2.1.3 URL Blocking

URL Blocking will block the webs containing pre-defined key words. This feature can filter both domain input suffix (like .com or .org, etc) and a keyword "bct" or "mpe".



3.2.1.3.1 Configuration

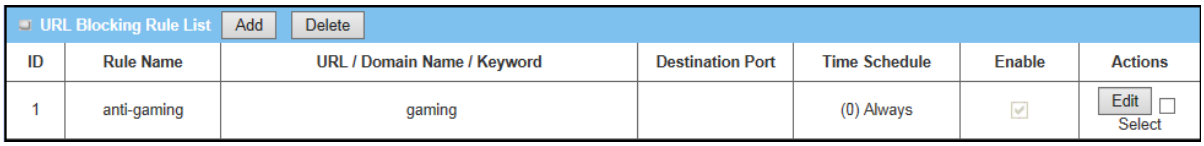


1. **URL Blocking**: Check the enable box if you want to activate URL Blocking function.
2. **Black List / White List**: Select one of the two filtering policies for the defined rules in URL Blocking Rule List.
   - Allow all to pass except those match the specified rules (Black List).
   - Deny all to pass except those match the specified rules (White List).
3. **Log Alert**: Enable the log alerting so that system will record URL blocking events when blocking rules are fired.
4. **Invalid Access Web Redirection**: Users will see a specific web page to know their access is blocked by rules.
5. **[Help]:** At the right upper corner of screen, one "[Help]" command let you see the on-line help message about URL Blocking function.

3.2.1.3.2 URL Blocking Rule List

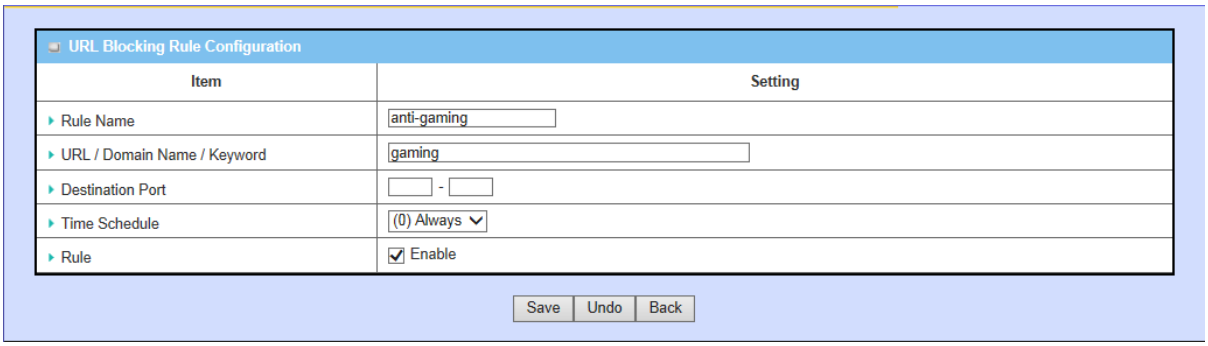
It is a list of all URL Blocking rules. You can add one new rule by clicking on the "Add"

command button. But also you can modify some existed URL blocking rules by clicking corresponding “Edit” command buttons at the end of each blocking rule in the URL Blocking Rule List. Besides, unnecessary rules can be removed by checking the “Select” box for those rules and then clicking on the “Delete” command button at the URL Blocking Rule List caption.



3.2.1.3.3 URL Blocking Rule Configuration

It supports the adding of one new rule or the editing of one existed rule. There are some parameters need to be specified in one URL blocking rule. They are Rule Name, URL / Domain Name / Keyword, Destination Port, Time Schedule and finally, the rule enable.

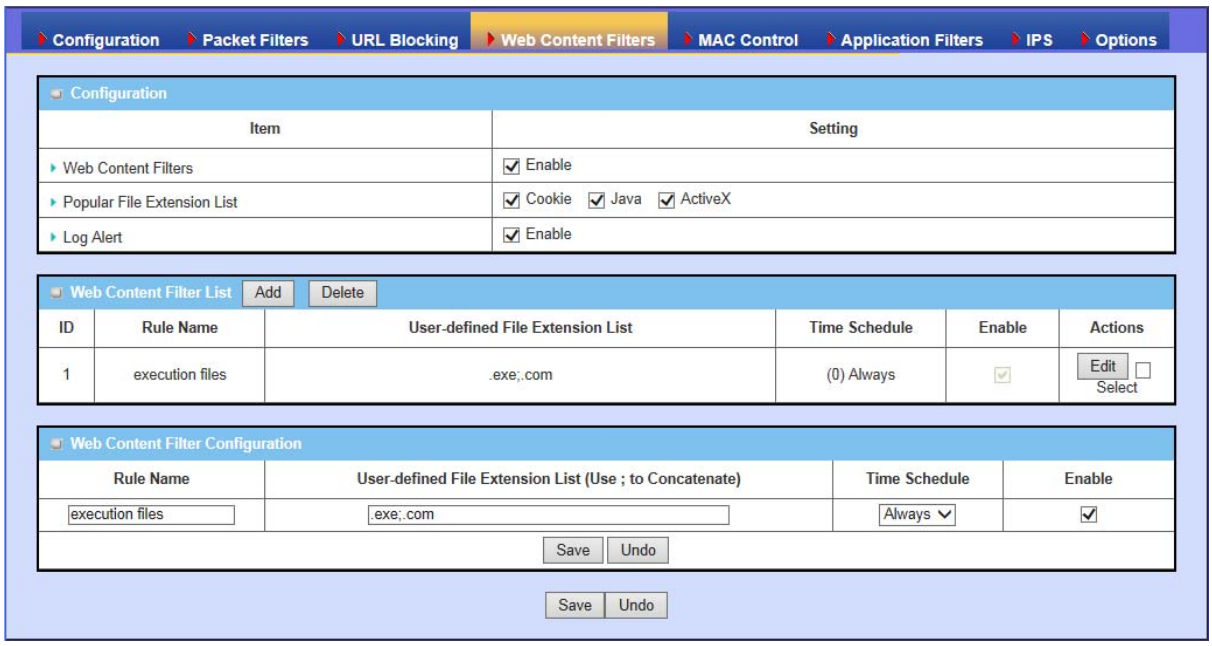


1. **Rule Name:** The name of URL blocking rule.
2. **URL/Domain Name/Keyword:** If any part of the Website's URL matches the pre-defined words, the connection will be blocked. You can enter up to 10 pre-defined words in a rule and each URL keyword is separated by ",", e.g., “google, yahoo, org”; In addition to URL keywords, it can also block the designated domain name, like “www.xxx.com“, “www.123aaa.org, mma.com”.
3. **Destination Port:** Specify the destination port in URL requests that want to be blocked in the URL blocking rule. You can define a single port (80) or a range of ports (1000-1999). An empty or “0” implies all ports are used.
4. **Time Schedule:** The rule can be turn on according to the schedule rule you specified, and give user more flexibility on access control. By default, it is always turned on when the rule is enabled. For more details, please refer to the **System -> Scheduling** menu.
5. **Rule Enable:** Check the enable box if you want to activate the rule. Each rule can be enabled or disabled individually.

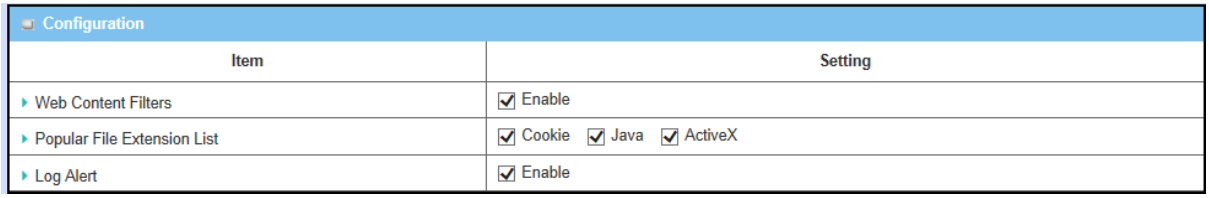
Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.2.1.4 Web Content Filters

Web Content Filters can block HTML requests with the specific extension file name, like ".exe", ".bat" (applications), "mpeg” (video), and block HTML requests with some script types, like Java Applet, Java Scripts, cookies and Active X.



3.2.1.4.1 Configuration

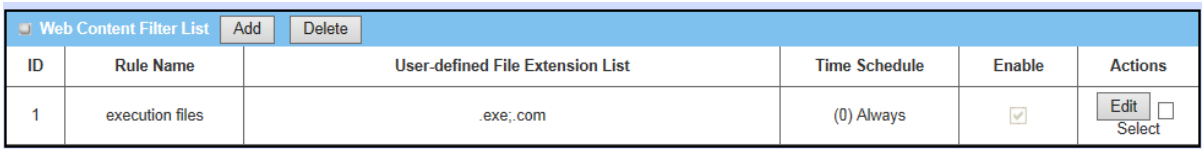


1. **Web Content Filters**: Check the Enable box if you want to enable Web Content Filters function.
2. **Popular File Extension List:** Check which extension types, Cookie, Java, ActiveX, are to be blocked.
3. **Log Alert**: Enable the log alerting so that system will record Web content filtering events when filtering rules are fired.

3.2.1.4.2 Web Content Filter Rule List

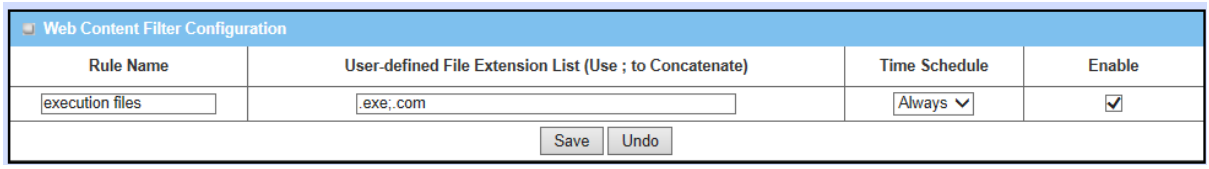
It is a list of all Web Content Filter rules. You can add one new rule by clicking on the “Add” command button. But also you can modify some existed Web Content Filter rules by clicking corresponding “Edit” command buttons at the end of each filtering

rule in the Web Content Filter List. Besides, unnecessary rules can be removed by checking the “Select” box for those rules and then clicking on the “Delete” command button at the Web Content Filter List caption.



3.2.1.4.3 Web Content Filter Configuration

It supports the adding of one new rule or the editing of one existed rule. There are some parameters need to be specified in one Web Content Filter rule. They are Rule Name, User-defined File Extension List, Time Schedule and finally, the rule enable.

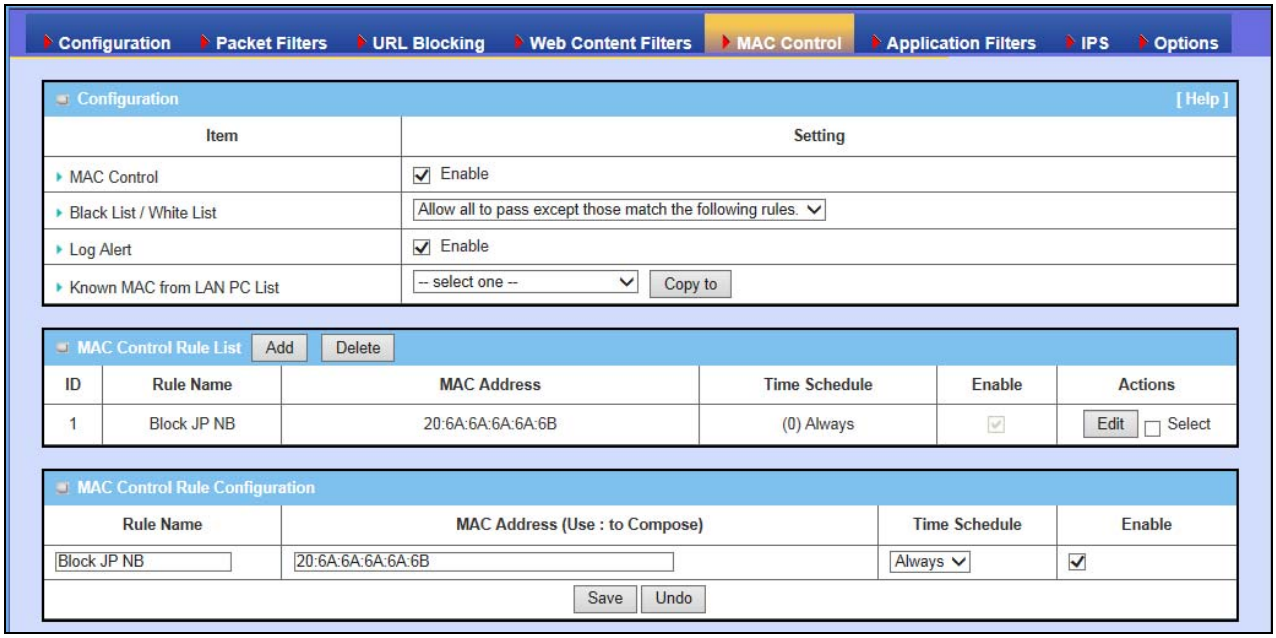


1. **Rule Name:** The name of Web Content Filter rule.
2. **User-defined File Extension List**: You can enter up to 10 file extensions to be blocked in a rule by using ‘;’ to concatenate these file extensions.
3. **Schedule:** The rule can be turn on according to the schedule rule you specified, and give user more flexibility on access control. By default, it is always turned on when the rule is enabled. For more details, please refer to the **System** -> **Scheduling** menu.
4. **Enable**: Check the box if you want to enable the rule. Each rule can be enabled or disabled individually.

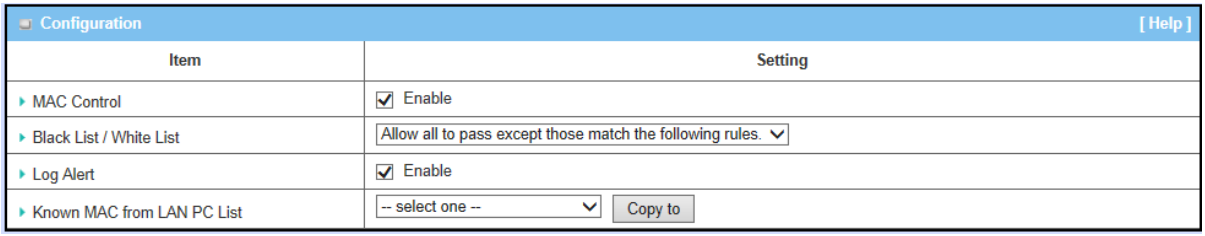
Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.2.1.5 MAC Control

MAC Control allows you to assign different access right for different users based on device’s MAC address.



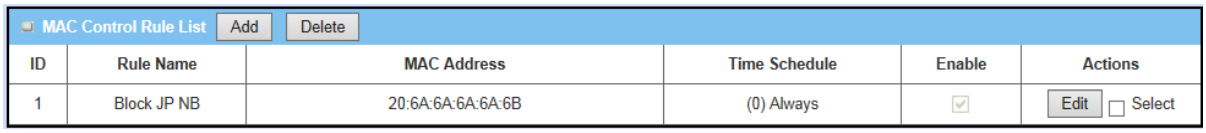
3.2.1.5.1 Configuration



1. **MAC Control**: Check the “Enable” box to activate the MAC Control function. All of the settings in this page will take effect only when “Enable” is checked.
2. **Black List / White List**: Select one of the two filtering policies for the defined rules.
   Black List - Allow all to pass except those match the specified rules.
   White List - Deny all to pass except those match the specified rules
3. **Log Alert**: Enable the log alerting so that system will record MAC control events when control rules are fired.
4. **Known MAC from LAN PC List**: You can see all of connected clients from this list, and copy their MAC address to the MAC Control Rule Configuration window below.

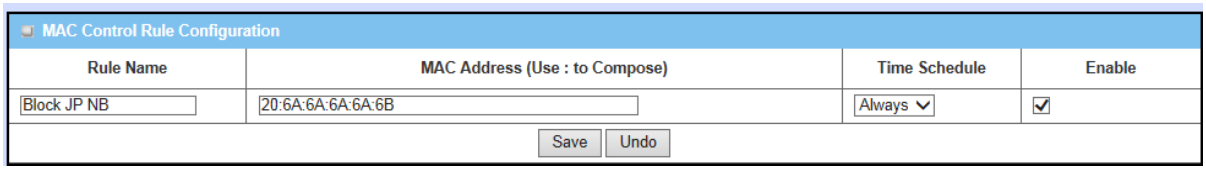
3.2.1.5.2 MAC Control Rule List

It is a list of all MAC Control rules. You can add one new rule by clicking on the “Add” command button. But also you can modify some existed MAC control rules by clicking corresponding “Edit” command buttons at the end of each control rule in the MAC Control Rule List. Besides, unnecessary rules can be removed by checking the “Select” box for those rules and then clicking on the “Delete” command button at the MAC Control Rule List caption.



3.2.1.5.3 MAC Control Rule Configuration

It supports the adding of one new rule or the editing of one existed rule. There are some parameters need to be specified in one MAC Control rule. They are Rule Name, MAC Address, Time Schedule and finally, the rule enable.



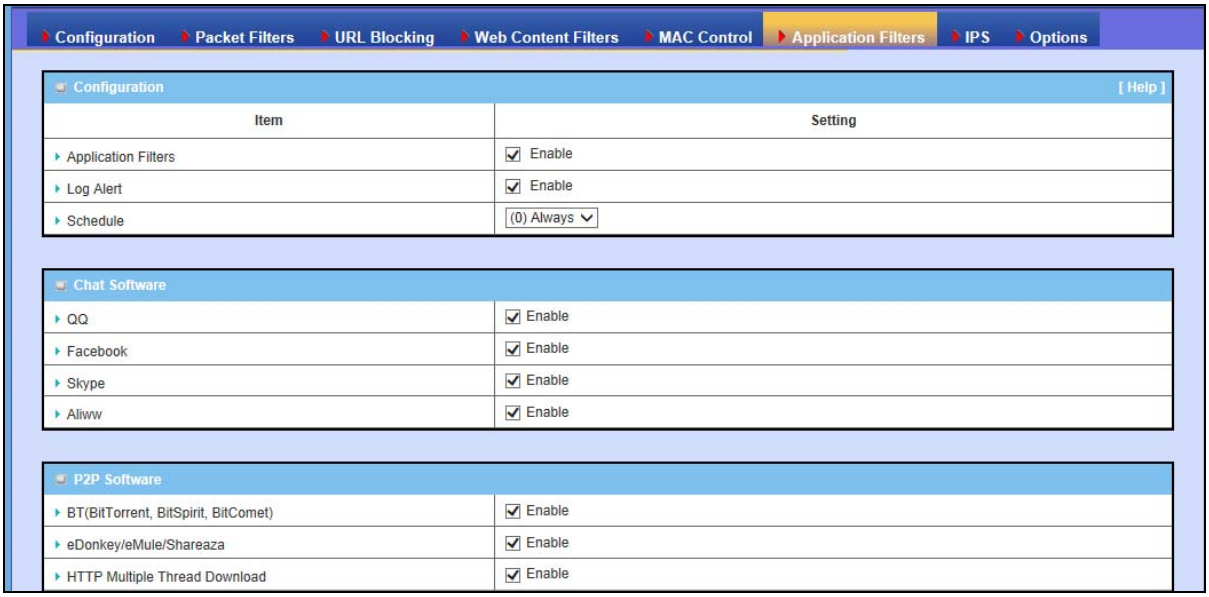
1. **Rule Name:** The name of Web Content Filter rule.
2. **MAC Address**: Input the MAC address of local device. You can input manually or copy it from **Known MAC from LAN PC List**. Please note the format of MAC address is like “xx:xx:xx:xx:xx:xx”. “x” is a hexadecimal digit.
3. **Schedule:** The rule can be turn on according to the schedule rule you specified, and give user more flexibility on access control. By default, it is always turned on when the rule is enabled. For more details, please refer to the **System** -> **Scheduling** menu.
4. **Enable**: Check the box if you want to enable the rule. Each rule can be enabled or disabled individually.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

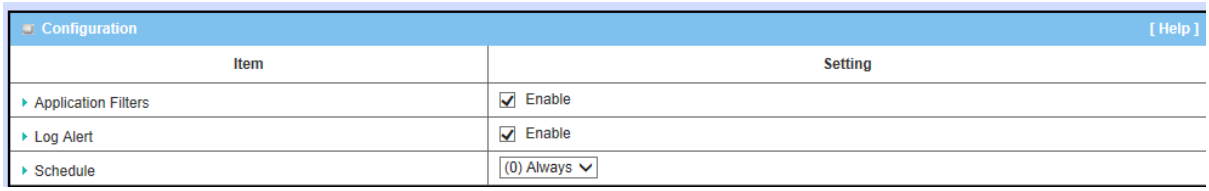
3.2.1.6 Application Filters

Application Filters can categorize Internet Protocol packets based on their application layer data and allow or deny their passing of gateway.

This device supports the application filters for various Internet chat software, P2P download, Proxy, and A/V streaming. You can select the applications to be blocked after the function is enabled, and specify the schedule rule for such Application Filters function.



3.2.1.6.1 Configuration

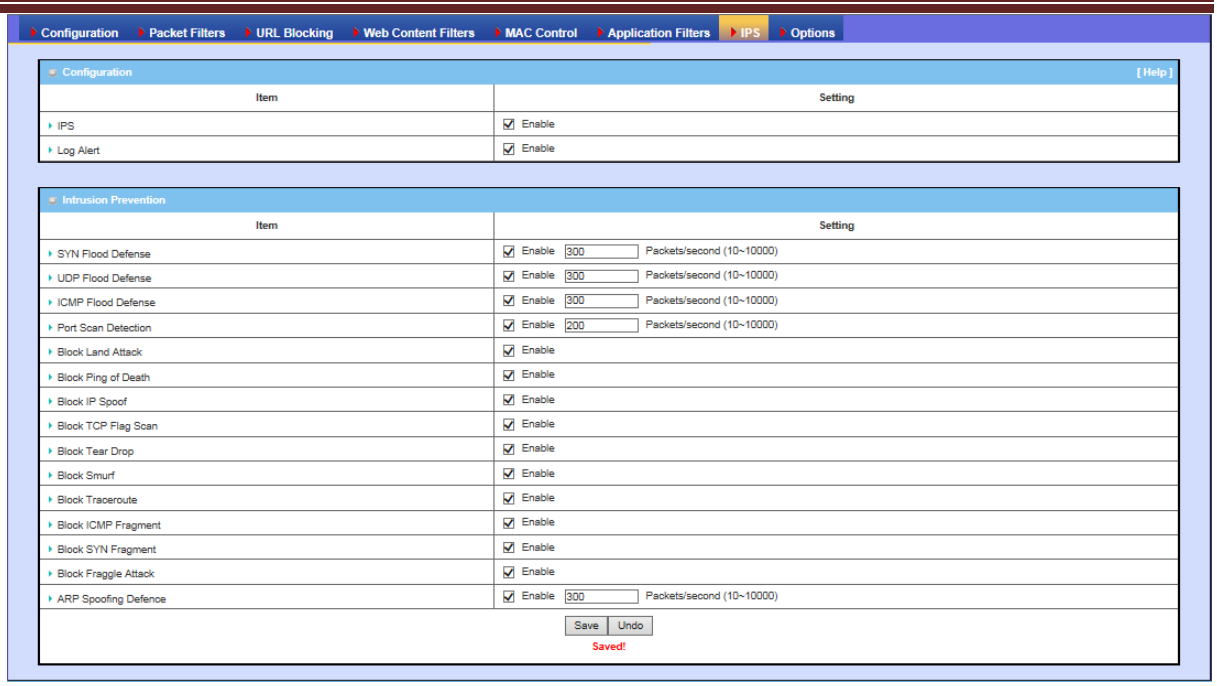


1. **Application Filters**: Check the “Enable” box to activate the Application Filters function. All of the settings in this page will take effect only when “Enable” is checked.
2. **Log Alert**: Enable the log alerting so that system will record Application Filter events when filtering rules are fired.
3. **Schedule:** All Application Filter rules can be turn on according to the schedule rule you specified, and give user more flexibility on access control. By default, they are always turned on when Application Filters function is enabled. For more details, please refer to the **System** -> **Scheduling** menu.

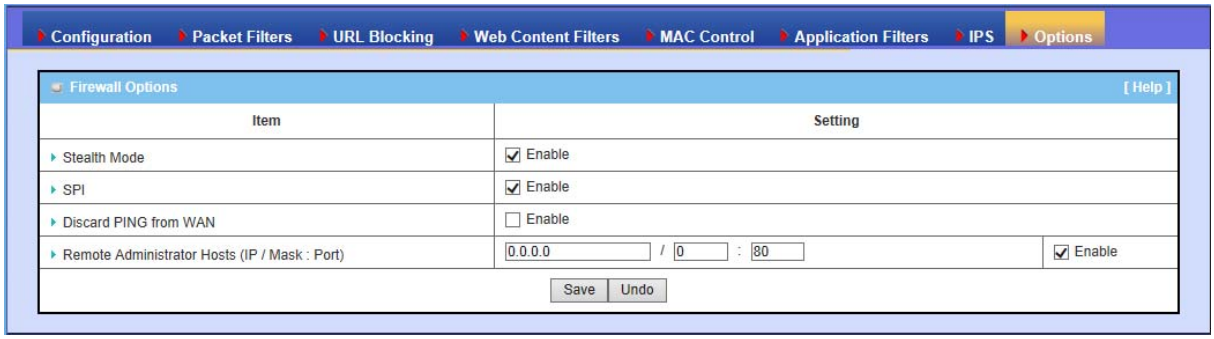
3.2.1.7 IPS

IPS (Intrusion Prevention Systems) are network security appliances that monitor network and/or system activities for malicious activity. The main functions of IPS are to identify malicious activity, log information about this activity, attempt to block/stop it and report it.

You can enable the IPS function and check the listed intrusion activities if necessary. There are some intrusion prevention items need a further Threshold parameter to work properly for intrusion detection. Besides, you can enable the log alerting so that system will record Intrusion events when corresponding intrusions are detected.



3.2.1.8 Options



1. **Stealth Mode:** Enable this feature, this device will not respond to port scans from the WAN so that makes it less susceptible to discovery and attacks on the Internet.
2. **SPI:** When this feature is enabled, the router will record the outgoing packet information pass through the router like IP address, port address, ACK, SEQ number and so on. And the router will check every incoming packet to detect if this packet is valid.
3. **Discard PING from WAN:** If this feature is enabled, this gateway won't reply any ICMP request packet from WAN side. It means any remote host can't get response when "ping" to this gateway. "Ping" is a useful command that we use to detect if a certain host is alive or not. But it also let hacker know about this. Therefore, many Internet servers will be set to ignore IGMP request.
4. **Remote Administrator Hosts (IP / Mask : Port):** In general, only local clients (LAN users) can browse the device's built-in web pages for device administration setting. This feature enables you to perform administration task from a certain

remote host. If this feature is enabled, only the specified IP address can perform remote administration. If the specified IP address is 0.0.0.0, any host can connect with this product to perform administration task. You can use subnet mask bits "/nn" notation to specified a group of trusted IP addresses. For example, "10.1.2.0/24".

NOTE: When Remote Administration is enabled, the web server port will be configured to 80 as default. You also can change web server port to other port

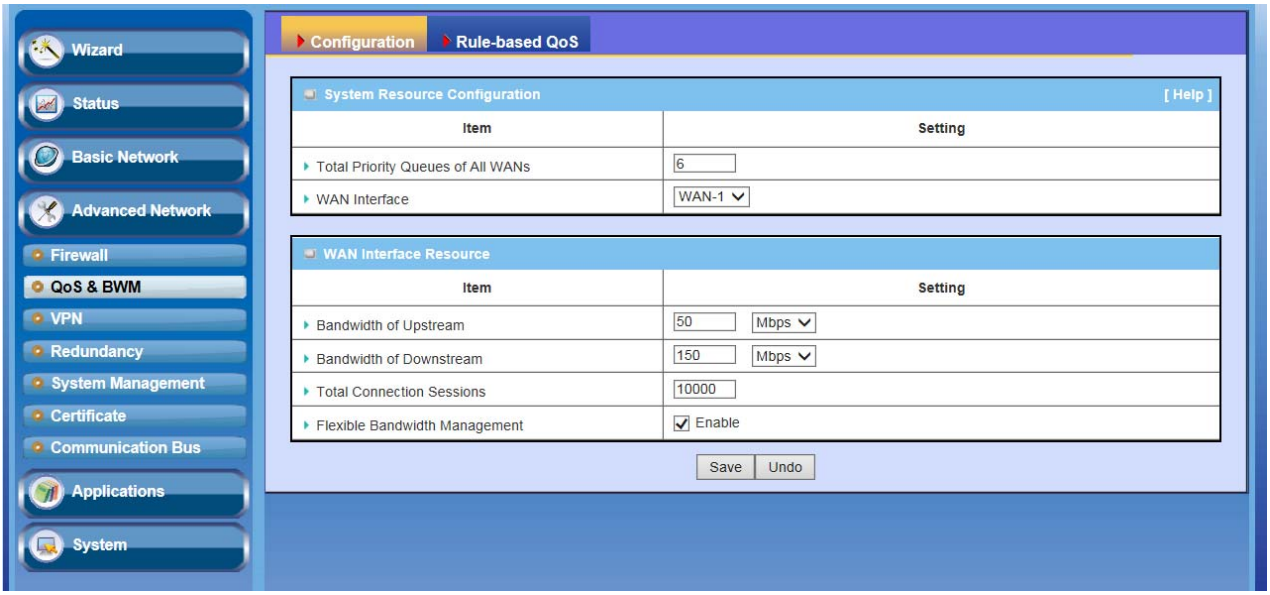
Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.2.2 QoS & BWM

The total amount of data traffic increases nowadays as the higher demand of mobile devices, like Game / Chat / VoIP / P2P / Video / Web access. In order to pose new requirements for data transport, e.g. low latency, low data loss, the entire network must ensure them via a connection service guarantee.

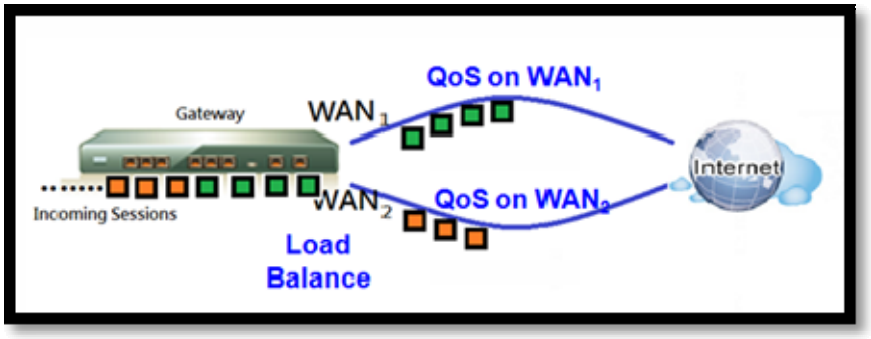
The main goal of QoS & BWM (Quality of Service and Bandwidth Management) is prioritizing incoming data, and preventing data loss due to factors such as jitter, delay and dropping. Another important aspect of QoS is ensuring that prioritizing one data flow doesn’t interfere with other data flows. So, QoS helps to prioritize data as it enters your router. By attaching special identification marks or headers to incoming packets, QoS determines which queue the packets enter, based on priority. This is useful when there are certain types of data you want to give higher priority to, such as voice packets given higher priority than Web data packets.

To utilize your network throughput completely, administrator must define bandwidth control rules carefully to balance the utilization of network bandwidth for all users to access. It is indeed required that an access gateway satisfies the requirements of latency-critical applications, minimum access right guarantee, fair bandwidth usage for same subscribed condition and flexible bandwidth management. Proroute Security Gateway provides a Rule-based QoS to carry out the requirements.

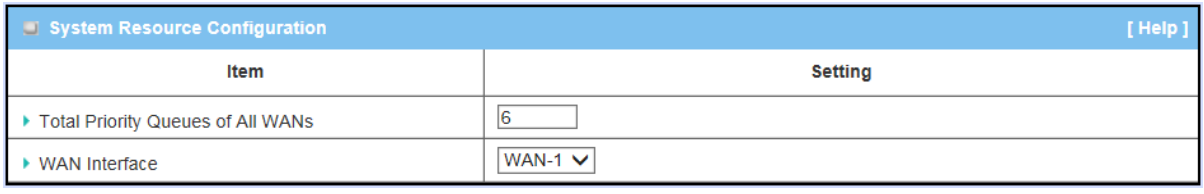


3.2.2.1 Configuration

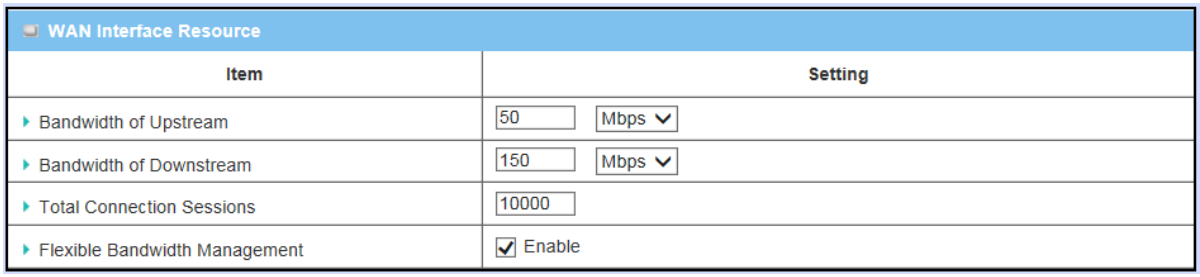
- **QoS on Multiple WAN Interfaces**
  - QoS on all WAN interfaces satisfies the requirements of latency-critical applications, minimum access right guarantee, fair bandwidth usage for same subscribed condition and flexible bandwidth management in a more flexible approach.
  - Integrated with Multi-WAN load balance function to maximize the total network throughput.



- **Flexible Bandwidth Management (FBM)**
  - Adjust the bandwidth distribution dynamically based on current bandwidth usage situation to get the maximum system network performance, and it is transparent to all users.



Before QoS & BWM function can work correctly, this gateway needs to define the resource for QoS & BWM function to utilize. They include the maximum number of priority queues that the device supports and some kinds of resources for each WAN interface. You can choose one WAN interface to define its resources, like available bandwidth of WAN connection and the number of total connection sessions. The application of Flexible Bandwidth Management on the interface can also be specified here.



1. **Bandwidth of Upstream:** The maximum bandwidth of uplink in Mbps.
2. **Bandwidth of Downstream:** The maximum bandwidth of downlink in Mbps.
3. **Total Connection Sessions:** Input the maximum number of connection sessions for the WAN interface**.**
4. **Flexible Bandwidth Management:** Apply flexible bandwidth management on the specific WAN interface by checking the Enable box.

3.2.2.2 Rule-based QoS

This gateway provides lots of flexible rules for you to set QoS policies. Basically, you need to know three parts of information before you create your own policies. First, “who” needs to be managed? Second, “what” kind of service needs to be managed? The last part is “how” you prioritize. Once you get this information, you can continue to learn more details in this section.

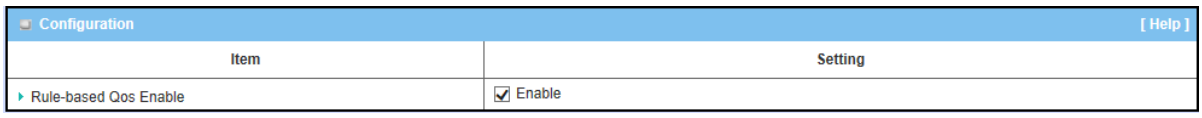
- **Flexible QoS Rule Definition**
  - Multiple Group Categories
    - Specify the group category in a QoS rule for the target objects that rule to be applied on.
    - Group Category can bases on VLAN ID, MAC Address, IP Address, Host Name or Packet Length. Category depends on model.
  - Differentiated Services
    - Specify the service type in a QoS rule for the target packets that rule to be applied on.
    - Differentiated services can be base on 802.1p, DSCP, TOS, VLAN ID, User-defined Services and Well-known Services.

- Well-known services include FTP(21), SSH(TCP:22), Telnet(23), SMTP(25), DNS(53), TFTP(UDP:69), HTTP(TCP:80), POP3(110), Auth(113), SFTP(TCP:115), SNMP&Traps(UDP:161-162), LDAP(TCP:389), HTTPS(TCP:443), SMTPs(TCP:465), ISAKMP(500), RTSP(TCP:554), POP3s(TCP:995), NetMeeting(1720), L2TP(UDP:1701) and PPTP(TCP:1723).

- Available Control Functions
  - There are 4 resources can be applied in a QoS rule: bandwidth, connection sessions, priority queues and DiffServ Code Point (DSCP). Control function that acts on target objects for specific services of packet flow is based on these resources.
  - For bandwidth resource, control functions include guaranteeing bandwidth and limiting bandwidth. For priority queue resource, control function is setting priority. For DSCP resource, control function is DSCP marking. The last resource is Connection Sessions; the related control function is limiting connection sessions.
- Individual / Group Control
  - One QoS rule can be applied to individual member or whole group in the target group. This feature depends on model.
- Outbound / Inbound Control
  - One QoS rule can be applied to the outbound or inbound direction of packet flow, even them both. This feature depends on model.

3.2.2.2.1 Configuration

It supports the activation of Rule-based QoS.



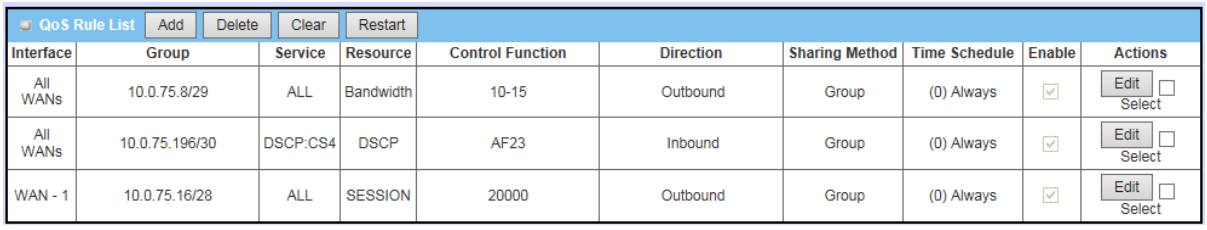
1. **Rule-based QoS Enable**: Check the box if you want to enable the QoS & BWM function.

Besides, at the right upper corner of screen, one “[Help]” command let you see the on-line help message about Rule-based QoS function.

3.2.2.2.2 QoS Rule List

It is a list of all QoS rules. You can add one new rule by clicking on the “Add” command button. But also you can modify some existed QoS rules by clicking corresponding “Edit” command buttons at the end of each rule in the QoS Rule List. Besides, unnecessary rules can be removed by checking the “Select” box for those

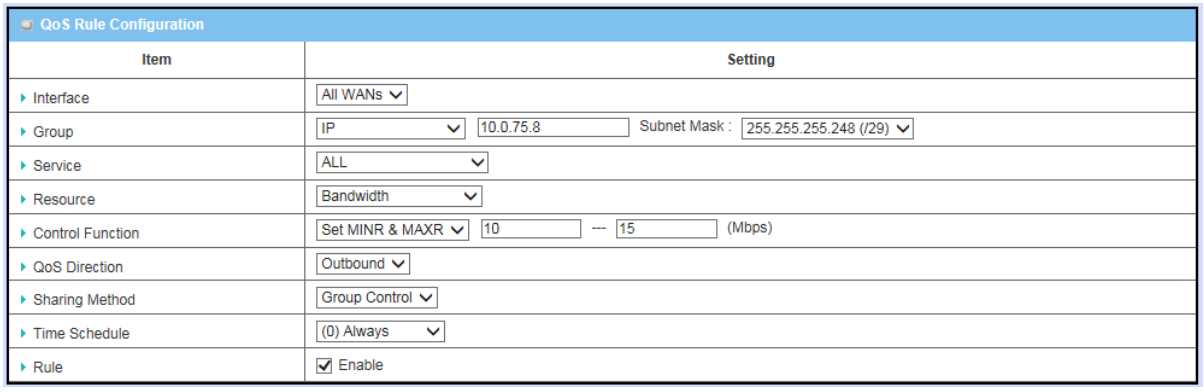
rules and then clicking on the “Delete” command button at the QoS Rule List caption. One “Clear” command button can let you clear all rules and “Restart” command button can let you restart the operation of all QoS rules.



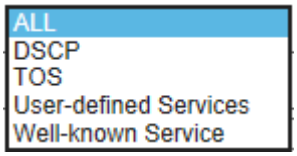
1. **Add:** After you enabled the rule-based QoS function, you can click on the “Add” button to create a new QoS rule.
2. **Delete:** After you selected some QoS rules by checking the “Select” box for each rule, you can click on the “Delete” button to remove those rules from the list.
3. **Clear:** Delete all existed QoS rules.
4. **Restart:** Press “Restart” button to re-initiate all QoS rules again.
5. **Edit:** Configure the specific QoS rule again.

3.2.2.2.3 QoS Rule Configuration

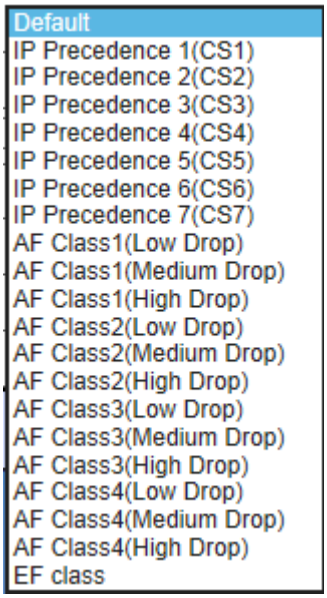
It supports the adding of one new rule or the editing of one existed rule. There are some parameters need to be specified in one QoS rule. They are Interface, Group, Service, Resource, Control Function, QoS Direction, Sharing Method, Time Schedule and finally, the rule enable.



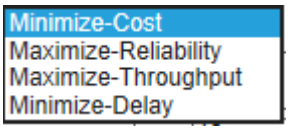
1. **Interface:** Select the WAN interface for the QoS rule.
2. **Group:** Specify the target client members for the rule by their VLAN ID, MAC Address, IP Address, Host Name or Group Object. These base categories depend on product models. Besides, “IP Address” group can be defined as an IP range with an IP address and its subnet mask. And “Group Object” is defined in the **System** -> **Grouping** menu. But what kinds of groups to use depend on product models.
3. **Service:** There are 5 options for service, including All, DSCP, TOS, User-defined Services and Well-known Service as below.



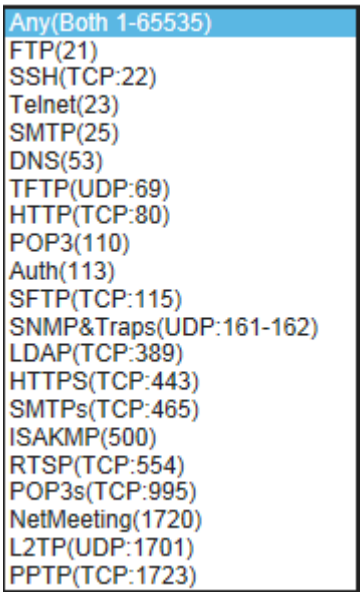
By default, it is “All”. It defines “what” kinds of service packets need to be managed. When “DSCP” is selected, another “DiffServ CodePoint” value must be specified. DSCP means DiffServ Code Point, as known as advanced TOS. You can choose this option if your local service gateway supports DSCP tags. The DSCP categories that this gateway can detect are as below.



You need to choose a correct one according to your device’s specification. When “TOS” is selected for Service, TOS value must be chosen from a list of 4 options. For example:



When “User-defined Services” is selected, two more parameters, Protocol Number and Service Port Range, must be defined. Protocol Number is either TCP or UDP or Both. Finally, when “Well-known Service” is selected, you can choose the well-known from a list like:



4. **Resource:** There are 4 resources can be chosen to control in the QoS rule. They are “Bandwidth”, “Connection Sessions”, “Priority Queues” and “DiffServ Code Points”.
5. **Control Function:** It depends on the chosen resource. For “Bandwidth” resource, the control function is “Set MINR & MAXR”. For “Connection Sessions”, the control function is “Set Session Limitation”. For “Priority Queues”, it is “Set Priority”. However, for “DiffServ Code Points”, it is “DSCP Marking” and you need specify the DSCP value additionally.
6. **QoS Direction:** Select the traffic direction to be applied for this rule.

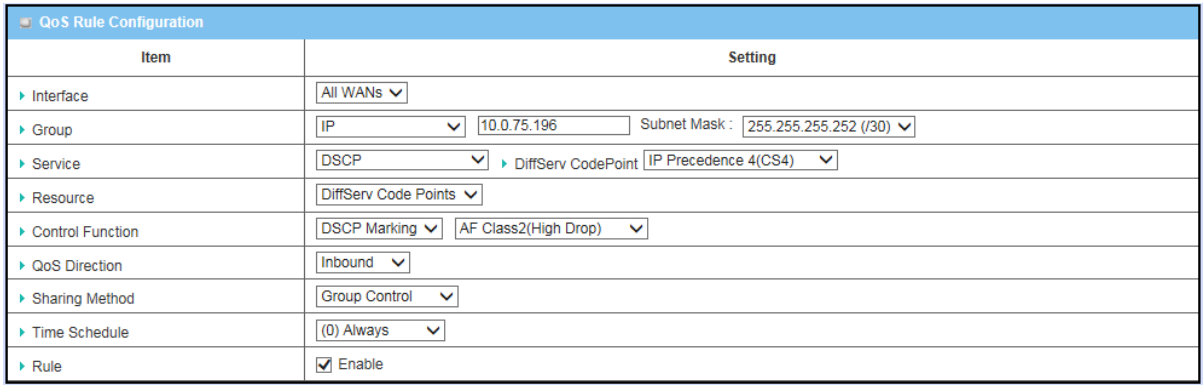
Direction	
IN	For Inbound data
OUT	For Outbound data
BOTH	Inbound and Outbound

7. **Sharing Method:** If you want to apply the value of control setting on each selected host in the “Group”, you need to select “Individual Control” for Sharing Method. On the other hand, if the value of control setting wants to be applied on all selected hosts in the “Group”, you need to select “Group Control”. For example, you define Control Function as “Set Session Limitation” and the limited sessions are 2000 sessions. You also define Sharing Method as “Individual Control”. Then, that means the maximum connection sessions of each selected host can’t exceed 2000 sessions. On the contrary, changing to “Group Control”, it means that group of client hosts totally can’t use over 2000 connection sessions.
8. **Schedule:** The rule can be turn on according to the schedule rule you specified, and give user more flexibility on access control. By default, it is always turned on when the rule is enabled. For more details, please refer to the **System** -> **Scheduling** menu.

9. **Enable**: Check the box if you want to enable the rule. Each rule can be enabled or disabled individually.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

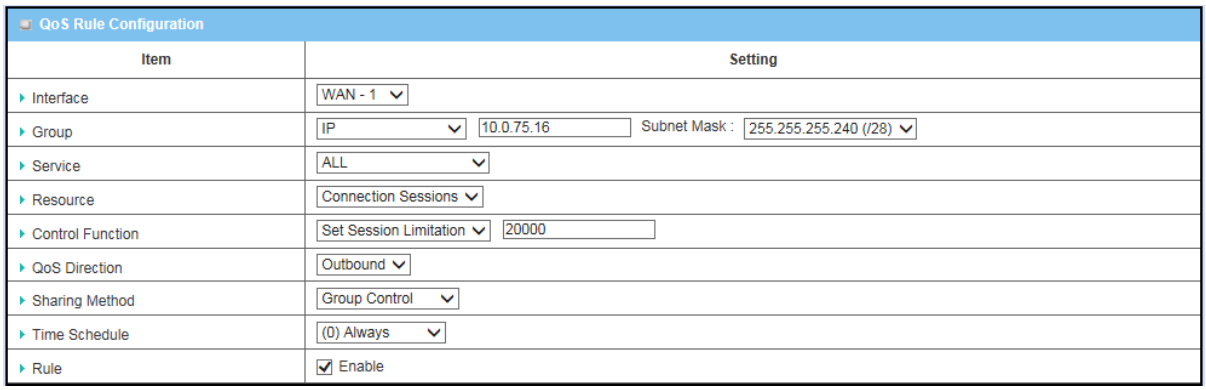
Example #1 for adding a “DSCP” type QoS rule



- Interface: Select “All WANs”.
- Group: Select “IP” and enter IP range: 10.0.75.196/30.
- Service: Select “DSCP” with DiffServ CodePoint is CS4.
- Resource: Select “DiffServ Code Points”.
- Control Function: Select “DSCP Marking” with “AF Class 2(High Drop)”.
- QoS Direction: Select “Inbound” for inbound traffic only.
- Sharing Method: Select “Group Control”.
- Schedule: Leave the default value of “(0) Always” as it is.

This rule means IP packets from all WAN interfaces to LAN IP address 10.0.75.196 ~ 10.0.75.199 which have DiffServ code points with “IP Precedence 4(CS4)” value will be modified by “DSCP Marking” control function with “AF Class 2(High Drop)” value at any time.

Example #2 for adding a “Connection Sessions” type QoS rule



- Interface: Select “WAN-1”.
- Group: Select “IP” and enter IP range: 10.0.75.16/28.

- Service: Select “ALL”.
- Resource: Select “Connection Sessions”.
- Control Function: Select “Set Session Limitation”, and set session number to 20000.
- QoS Direction: Select “Outbound” for outbound traffic only. It is for the client devices under the gateway to establish multiple sessions with servers in the Internet.
- Sharing Method: Select “Group Control”.
- Schedule: Leave the default value of “(0) Always” as it is.

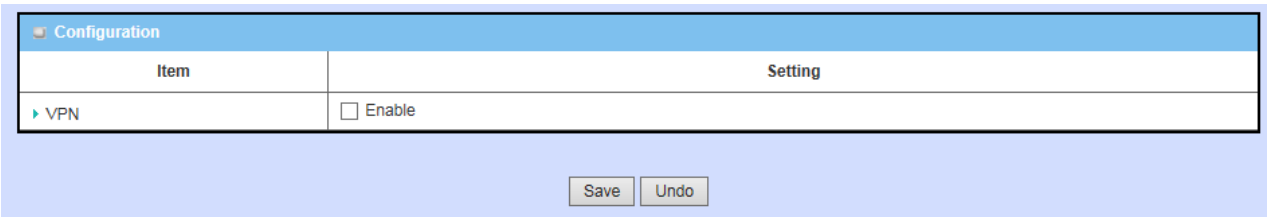
This rule defines that all client hosts, whose IP address is in the range of 10.0.75.16~31, can access to the Internet and keep a maximum 20000 connection sessions totally at any time.

3.2.3 VPN Setup

A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefitting from the functionality, security and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two. The tunnel technology supports data confidentiality, data origin authentication and data integrity of network information by utilizing encapsulation protocols, encryption algorithms, and hashing algorithms.

The product series supports following tunneling technologies to establish secure tunnels between multiple sites for data transferring, including IPSec, PPTP, L2TP (over IPSec) and GRE. Advanced functions include Full Tunnel, Tunnel Failover, Tunnel Load Balance, NetBIOS over IPSec, NAT Traversal and Dynamic VPN.

3.2.3.1 Configuration



To enable the VPN function, you should go to Configuration before any setting.

3.2.3.2 IPSec

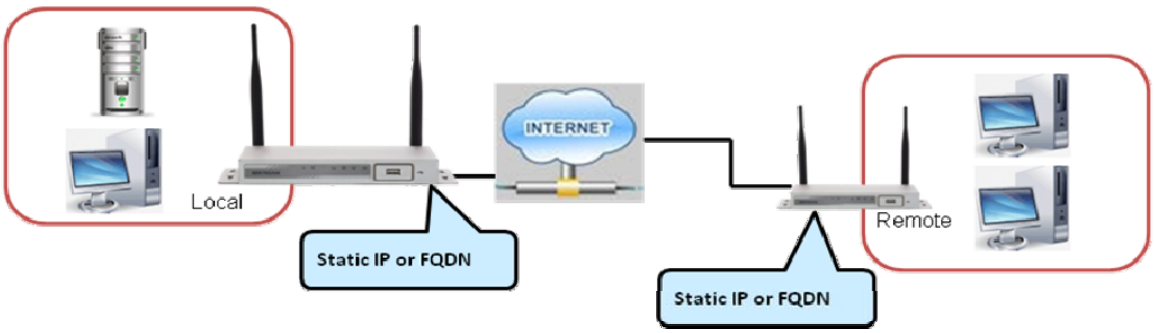
Internet Protocol Security (IPSec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPSec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session.

An IPSec VPN tunnel is established between IPSec client and server. Sometimes, we call the IPSec VPN client as the initiator and the IPSec VPN server as the responder. There are two phases to negotiate between the initiator and responder during tunnel establishment, IKE phase and IPSec phase. At IKE phase, IKE authenticates IPSec peers and negotiates IKE SAs (Security Association) during this phase, setting up a secure channel for negotiating IPSec SAs in phase 2. At IPSec phase, IKE negotiates IPSec SA parameters and sets up matching IPSec SAs in the peers. After these both phases, data is transferred between IPSec peers based on the IPSec parameters and keys stored in the SA database.

3.2.3.2.1 IPSec VPN Tunnel Scenarios

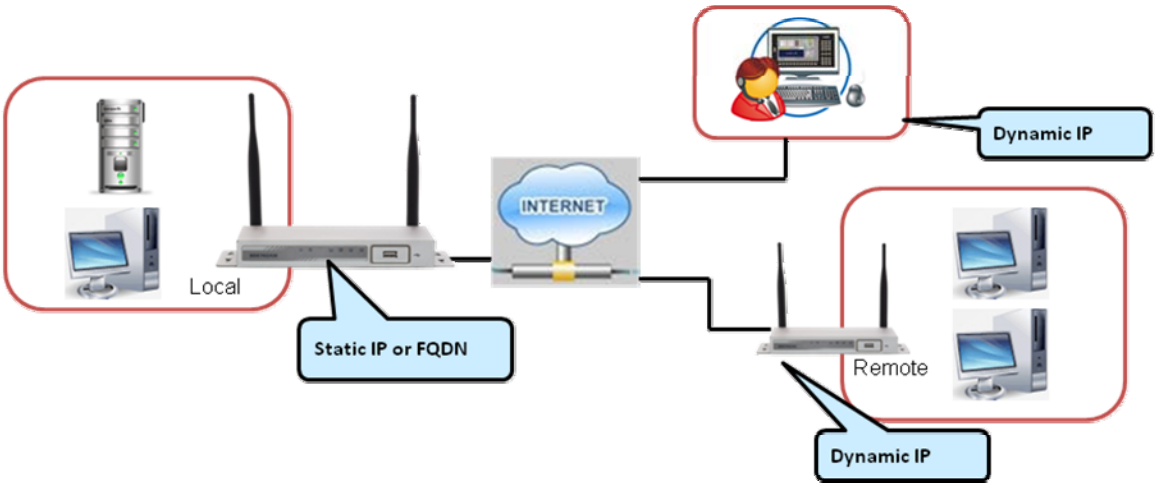
There are some common IPSec VPN connection scenarios as follows:

- Site to Site
  The device establishes IPSec VPN tunnels with security gateway in headquarters or branch offices. Either local or remote peer gateway which can be recognized by a static IP address or a FQDN can initiate the establishing of an IPSec VPN tunnel. Two peers of the tunnel have their own Intranets and the secure tunnel serves for data communication between these two subnets of hosts.



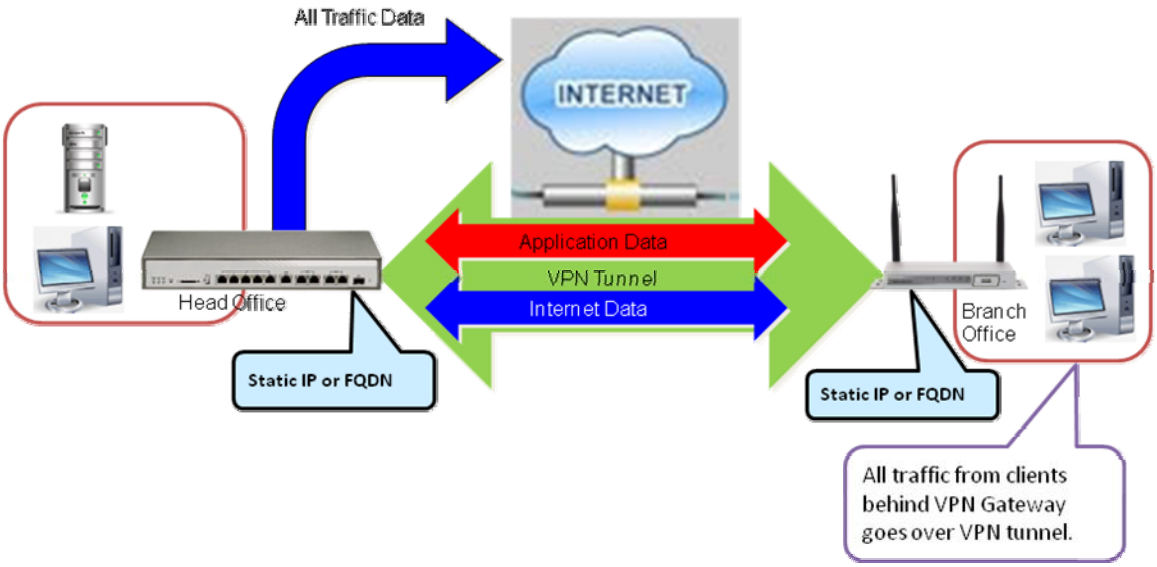
- Dynamic VPN
  Business Security Gateway can ignore IP information of clients when using Dynamic VPN, so it is suitable for users to build VPN tunnels with Business Security Gateway from a remote mobile host or mobile site. Remote peer is a host or a site will be indicated in the negotiation packets, including what remote subnet

is. It must be noted that the remote peer has to initiate the tunnel establishing process first in this application scenario.

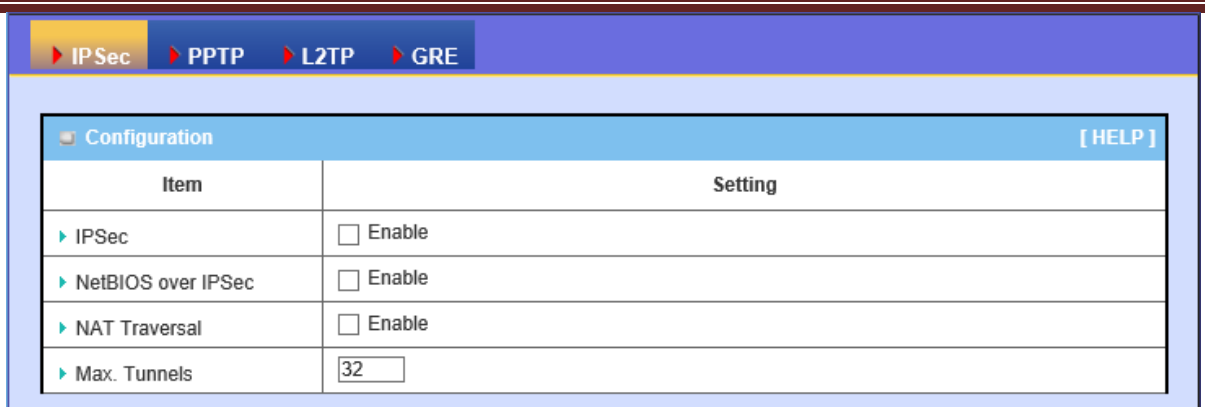


There is one more advanced IPSec VPN application:

- Site to Site – Support Full Tunnel Application
  When Full Tunnel function of remote Business Security Gateway is enabled, all data traffic from remote clients behind remote Business Security Gateway will goes over the VPN tunnel. That is, if a user is operating at a PC that is in the Intranet of remote Business Security Gateway, all application packets and private data packets from the PC will be transmitted securely in the VPN tunnel to access the resources behind local Business Security Gateway, including surfing the Internet. As a result, every time the user surfs the web for shopping or searching data on Internet, checking personal emails, or accessing company servers, all are done in a secure way through local Business Security Gateway.



3.2.3.2.2 IPSec Configuration

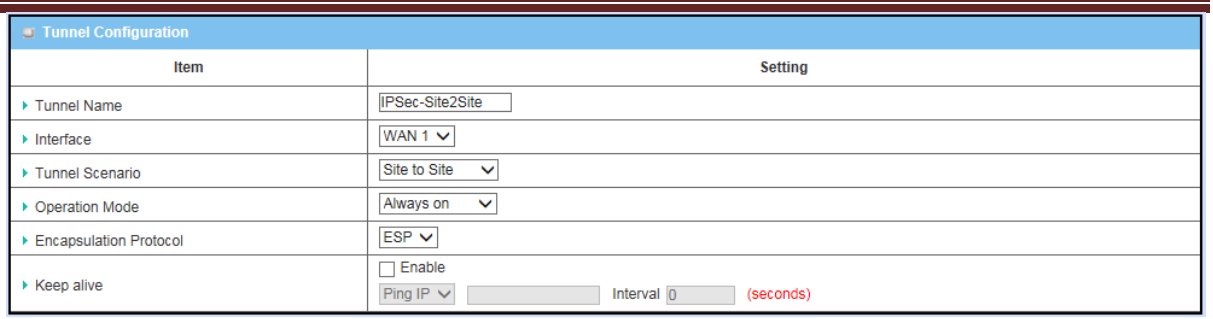


1. **IPSec:** You could trigger the function of IPSec VPN if you check “Enable” box.
2. **NetBIOS over IPSec:** If you would like two Intranets behind two Business Security Gateways to receive the NetBIOS packets from Network Neighborhood, you have to check “Enable” box.
3. **NAT Traversal:** Some NAT routers will block IPSec packets if they don’t support IPSec pass through. If your Business Security Gateway connects to this kind of NAT router which doesn’t support IPSec pass through, you need to activate this option in your Business Security Gateway.
4. **Max. Tunnels:** The device supports up to 32 IPSec tunnels, but you can specify it with the number of maximum current activated IPSec tunnels that is smaller or equal to 32.
5. You can add new, edit or delete some IPSec tunnels in Tunnel List & Status as follows.

3.2.3.2.3 Tunnel List & Status

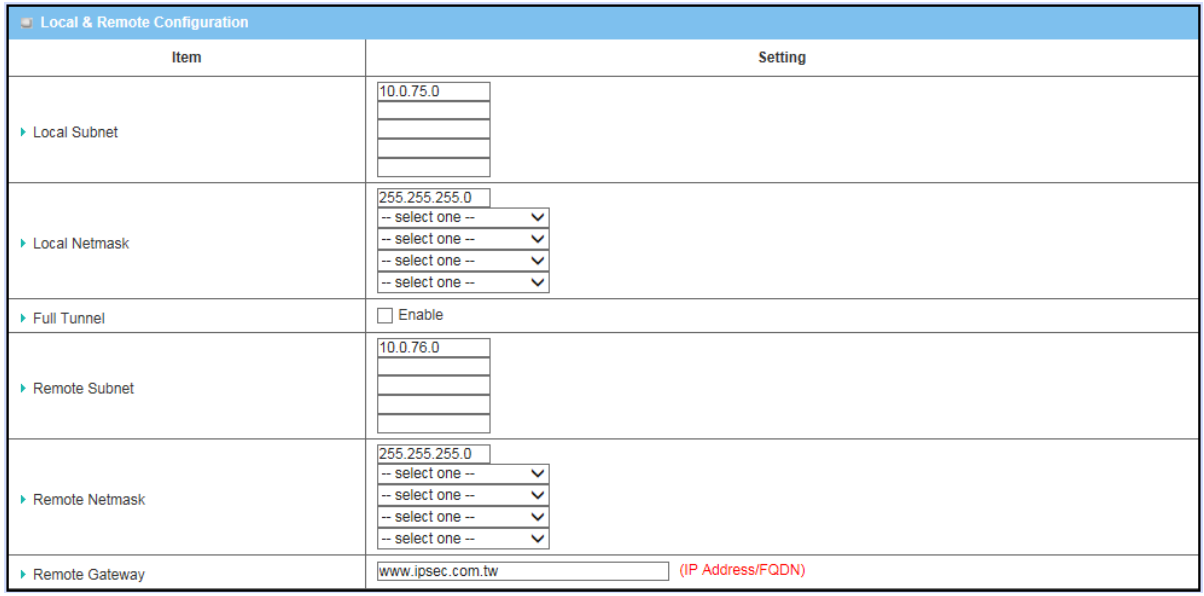
1. **Add:** You can add one new IPSec tunnel with Site to Site scenario by clicking the “Add” button.
2. **Delete:** Delete selected tunnels by checking the “Select” box at the end of each tunnel list and then clicking the “Delete” button.
3. **Refresh:** To refresh the Tunnel List & Status each 2 seconds by clicking on the “Refresh” button.
4. **Tunnel:** Check the “Enable” box to activate the IPSec tunnel.
5. **Edit:** You can edit one tunnel configuration by clicking the “Edit” button at the end of each tunnel list.

3.2.3.2.4 Tunnel Configuration



1. **Tunnel Name:** Enter the name of tunnel.
2. **Interface:** Decide the WAN Interface to establish the tunnel.
3. **Tunnel Scenario:** Support “Site to Site”, “Site to Host”, “Host to Site”, “Host to Host” and “Dynamic VPN”. Select one from them.
4. **Operation Mode:** Default is “Always on” and other options depend on product models.
5. **Encapsulation Protocol**: Default is ESP and other options depend on product models.
6. **Keep-alive:** Check “Enable” box to keep alive the tunnel. By default, keep-alive method is “Ping IP” and other options depend on product models. Input the IP address of remote host that exists in the opposite side of the VPN tunnel (Ex. You can input the LAN IP address of remote Business Security Gateway). The Interval is specified with the time interval between two ping requests, and by default, it is 30 seconds. Now, the device will start to ping remote host when there is no traffic within the VPN tunnel. If the device can't get ICMP response from remote host anymore, it will terminate the VPN tunnel automatically.

3.2.3.2.5 Local & Remote Configuration

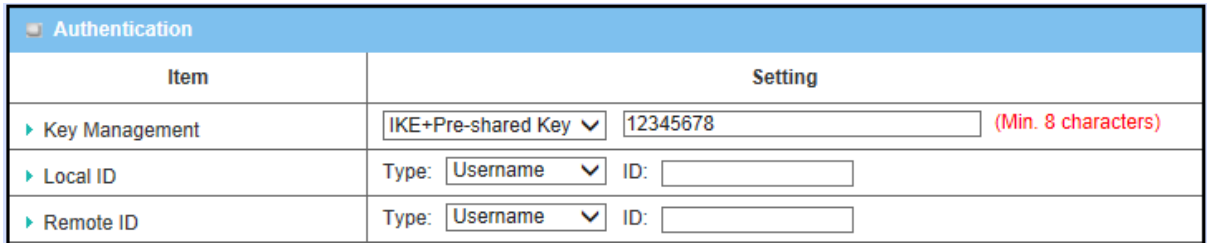


1. **Local Subnet:** The subnet of LAN site of local Business Security Gateway. It can be a host, a partial subnet, or the whole subnet of LAN site of local gateway.

There are 5 entries for Local Subnet.

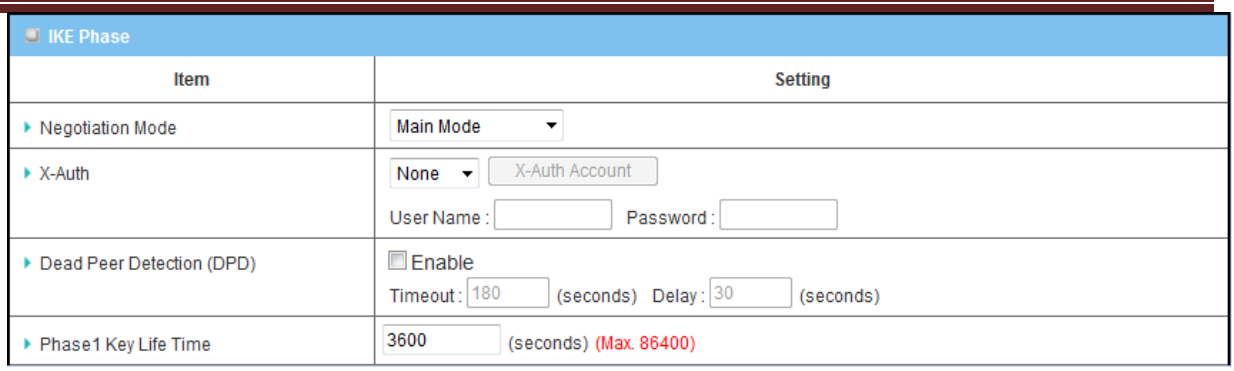
2. **Local Netmask:** The local netmask and associated local subnet can define a subnet domain for the local devices connected via the VPN tunnel. There are 5 entries for Local Netmask.
3. **Full Tunnel:** All traffic from Intranet of Business Security Gateway goes over the IPSec VPN tunnel if these packets don't match the Remote Subnet of other IPSec tunnels. That is, both application data and Internet access packets land up at the VPN concentrator.
4. **Remote subnet:** The subnet of LAN site of remote Business Security Gateway. It can be a host, a partial subnet, or the whole subnet of LAN site of remote gateway. There are 5 entries for Remote Subnet.
5. **Remote Netmask:** The remote netmask and associated remote subnet can define a subnet domain for the remote devices connected via the VPN tunnel. There are 5 entries for Remote Netmask.
6. **Remote Gateway:** Enter the IP address or FQDN of remote Business Security Gateway.

3.2.3.2.6 Authentication



1. **Key Management:** Select "IKE+Pre-shared Key" or "Manually". Other options depend on product models. By default, "IKE+Pre-shared Key" method is adopted for key management. It is the first key used in IKE phase for both VPN tunnel initiator and responder to negotiate further security keys to be used in IPSec phase. The pre-shared key must be the same for both VPN tunnel initiator and responder. When "Manually" key management is adopted, the Pre-shared is not necessary.
2. **Local ID:** The Type and the Value of the local Business Security Gateway must be the same as that of the Remote ID of the remote VPN peer. There are 4 types for Local ID: User Name, FQDN, User@FQDN and Key ID.
3. **Remote ID:** The Type and the Value of the local Business Security Gateway must be the same as that of the local ID of the remote VPN peer. There are also 4 types for Remote ID: User Name, FQDN, User@FQDN and Key ID.

3.2.3.2.7 IKE Phase



1. **Negotiation Mode:** Choose Main Mode or Aggressive Mode:
   Main Mode provides identity protection by authenticating peer identities when pre-shared keys are used. The IKE SA's are used to protect the security negotiations. Aggressive mode will accelerate the establishing speed of VPN tunnel, but the device will suffer from less security in the meanwhile. Hosts in both ends of the tunnel must support this mode so as to establish the tunnel properly.
2. **X-Auth:** For the extended authentication function (XAUTH), the VPN client (or initiator) needs to provide additional user information to the remote VPN server (or Business Security Gateway). The VPN server would reject the connect request from VPN clients because of invalid user information, even though the pre-shared key is correct. This function is suitable for remote mobile VPN clients. You can not only configure a VPN rule with a pre-shared key for all remote users, but you can also designate account / password for specific users that are permitted to establish VPN connection with VPN server. There are 3 roles to let Business Security Gateway behave as for X-Auth authentication, including None, Server and Client. For None role, there is no X-Auth authentication happens during VPN tunnel establishing. For Server role, click "X-Auth Account" button to modify 10 user accounts for user validation during tunnel establishing to VPN server. Finally, for Client role, there are two additional parameters to fill: "User Name" and "Password" for valid user to initiate that tunnel.
3. **Dead Peer Detection:** This feature will detect if remote VPN peer still exists. Delay indicates the interval between detections, and Timeout indicates the timeout of detected to be dead.
4. **Phase 1 Key Life Time**: The value of life time represents the life time of the key which is dedicated at Phase 1 between both end gateways.

3.2.3.2.8 IKE Proposal Definition

IKE Proposal Definition

ID	Encryption	Authentication	DH Group	Definition
1	AES-auto	SHA1	Group 2	Enable
2	AES-auto	MD5	Group 2	Enable
3	DES	SHA1	Group 2	Enable
4	3DES	SHA1	Group 2	Enable

There are 4 IKE proposals can be defined by you and used in IKE phase of negotiation between two VPN peers.

1. **Encryption:** There are six algorithms can be selected: DES, 3DES, AES-auto, AES-128, AES-192, and AES-256.
2. **Authentication:** There are **five** algorithms can be selected: None, MD5, SHA1, SHA2-256 and SHA2-512.
3. **DH Group:** There are **nine** groups can be selected: None, Group 1 (MODP768), Group 2 (MODP1024), Group 5 (MODP1536) and Group14 ~ 18.
4. **Enable:** Check this box to enable the IKE Proposal during tunnel establishing.

3.2.3.2.9 IPSec Phase

IPSec Phase

Item	Setting
Phase2 Key Life Time	28800 seconds (Max. 86400)

1. **Phase 2 Key Life Time**: The value of life time represents the life time of the key which is dedicated at Phase 2 between two VPN peers.

3.2.3.2.10 IPSec Proposal Definition

IPSec Proposal Definition

ID	Encryption	Authentication	PFS Group	Definition
1	AES-auto	SHA1	Group 2	Enable
2	AES-auto	MD5		Enable
3	DES	SHA1		Enable
4	3DES	SHA1		Enable

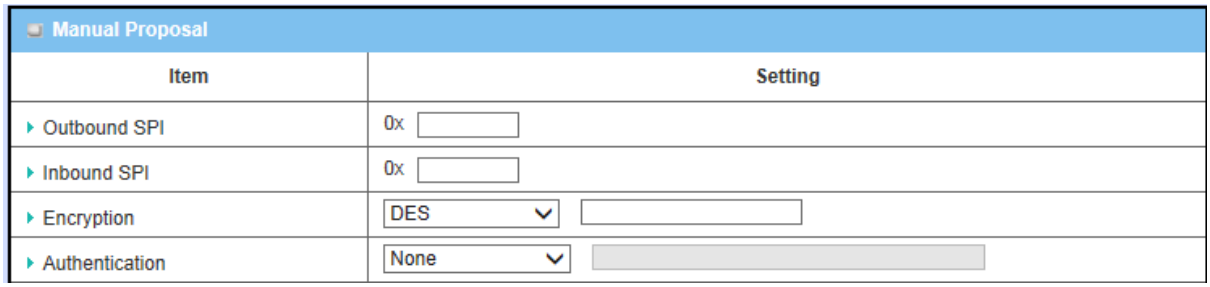
There are 4 IPSec proposals can be defined by you and used in IPSec phase of negotiation between two VPN peers.

1. **Encryption:** There are six algorithms can be selected: DES, 3DES, AES-auto, AES-128, AES-192, and AES-256.
2. **Authentication:** There are five algorithms can be selected: None, MD5, SHA1, SHA2-256 and SHA2-512.
3. **PFS Group:** There are nine groups can be selected: None, Group 1 (MODP768),

Group 2 (MODP1024), Group 5 (MODP1536) and Group14 ~ 18. Once the PFS Group is selected in one IPSec proposal, the one in other 3 IPSec proposals uses the same choice.

4. **Enable:** Check this box to enable the IKE Proposal during tunnel establishing.

3.2.3.2.11 Manual Proposal



When “Manually” key management is used, there are 4 further parameters need to be specified by you and used in IPSec tunnel establishing.

1. **Outbound SPI:** SPI is an important parameter during hashing. Outbound SPI will be included in the outbound packet transmitted from local gateway. The value of outbound SPI should be set in hex formatted.
2. **Inbound SPI:** Inbound SPI will be included in the inbound packet transmitted from remote VPN peer. It will be used to de-hash the coming packet and check its integrity. The value of inbound SPI should be set in hex formatted.
3. **Encryption Algorithm:** There are five algorithms can be selected: DES, 3DES, AES-128, AES-192, and AES-256. Encryption key is used by the encryption algorithm. Its length is 16 in hex format if encryption algorithm is DES or 48 if 3DES. However, AES-128 uses 32 length of hex format, AES-192 uses 48 length of hex format, and AES-256 uses 64 length of hex format. The key value should be set in hex formatted here.
4. **Authentication:** There are five algorithms can be selected: None, MD5, SHA1, SHA2-256 and SHA2-512. Authentication key is used by the authentication algorithm and its length is 32 in hex format if authentication algorithm is MD5 or 40 if SHA1. However, SHA2-256 uses 64 length of hex format. Certainly, its length will be 0 if no authentication algorithm is chosen. The key value should be also set in hex formatted.

3.2.3.3 PPTP

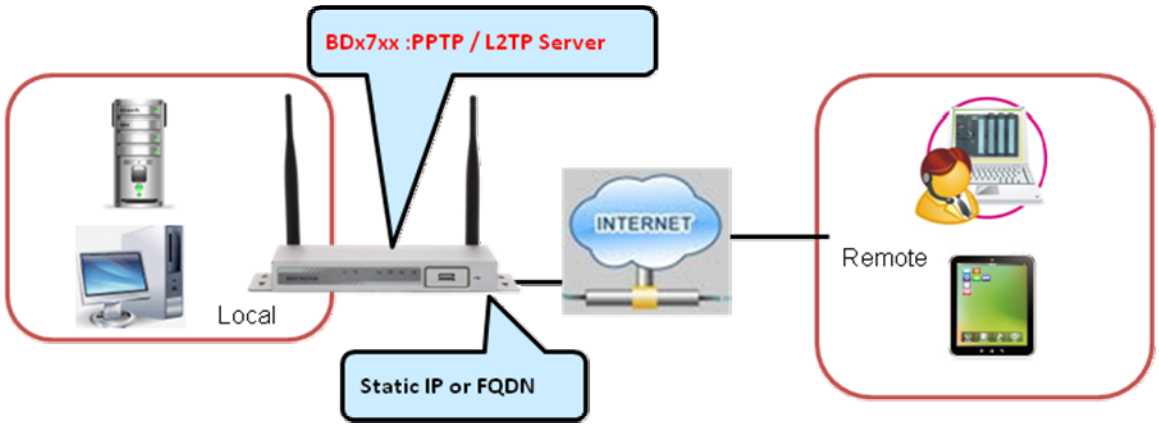
The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks. PPTP uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets. The PPTP specification does not describe encryption or authentication features and relies on the Point-to-Point Protocol being tunneled to

implement security functionality. However, the most common PPTP implementation shipping with the Microsoft Windows product families implements various levels of authentication and encryption natively as standard features of the Windows PPTP stack. The intended use of this protocol is to provide security levels and remote access levels comparable with typical VPN products.

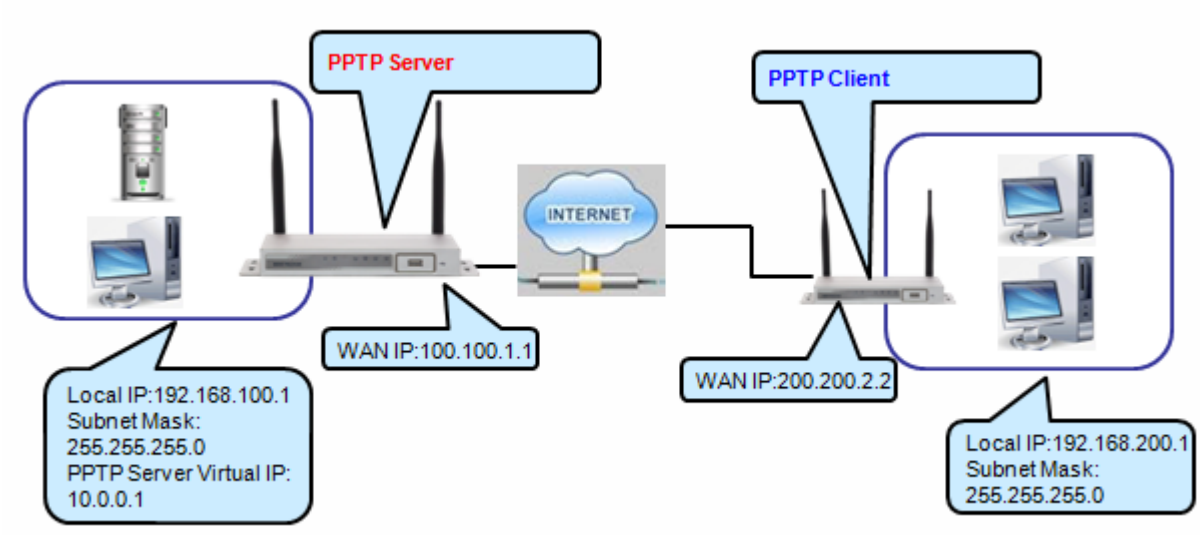
3.2.3.3.1 PPTP / L2TP VPN Tunnel Scenarios

There are some common PPTP/L2TP VPN connection scenarios as follows:

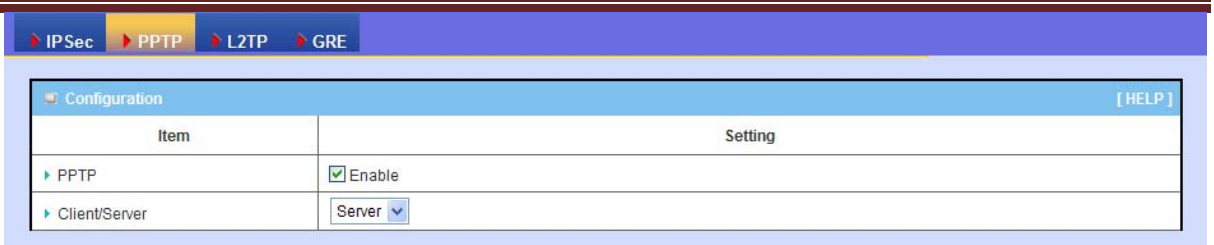
- PPTP / L2TP Server for Remote Mobile Users
  The device acts as Server role for remote users to dial in and shares some services in Intranet for them.



- PPTP / L2TP Server / Client Application
  The device acts as Server or Client role in SMB Headquarters or Branch Office.



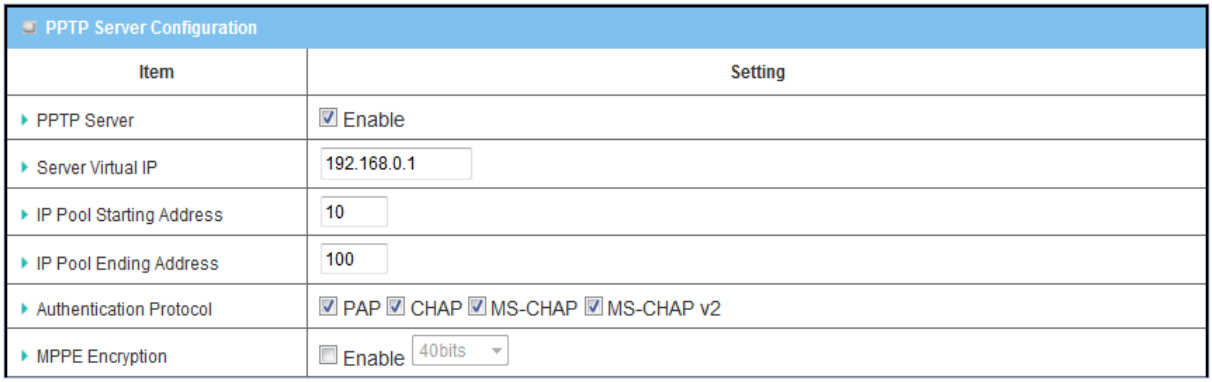
The Business Security Gateway can behave as a PPTP server and a PPTP client at the same time.



1. **PPTP:** Check the “Enable” box to activate PPTP client and server functions.
2. **Client/Server:** Choose Server or Client to configure corresponding role of PPTP VPN tunnels for the Business Security Gateway beneath the choosing screen

3.2.3.3.2 PPTP Server Configuration

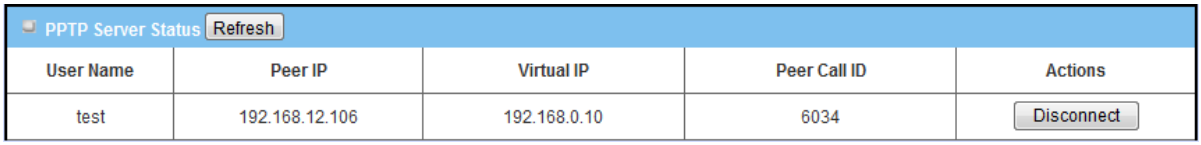
The Business Security Gateway can behave as a PPTP server, and it allows remote hosts to access LAN servers behind the PPTP server. The device can support four authentication methods: PAP, CHAP, MS-CHAP and MS-CHAP v2. Users can also enable MPPE encryption when using MS-CHAP or MS-CHAP v2.



1. **PPTP Server:** Enable or disable PPTP server function.
2. **Server Virtual IP:** It is the virtual IP address of PPTP server used in PPTP tunneling. This IP address should be different from the gateway one and members of LAN subnet of Business Security Gateway.
3. **IP Pool Starting Address:** This device will assign an IP address for each remote PPTP client. This value indicates the beginning of IP pool.
4. **IP Pool Ending Address:** This device will assign an IP address for each remote PPTP client. This value indicates the end of IP pool.
5. **Authentication Protocol:** You can choose authentication protocol as PAP, CHAP, MS-CHAP, or MS-CHAP v2.
6. **MPPE Encryption:** Check the “Enable” box to activate MPPE encryption. Please note that MPPE needs to work with MS-CHAP or MS-CHAP v2 authentication method. In the meantime, you also can choose encryption length of MPPE encryption, 40 bits, 56 bits or 128 bits.

3.2.3.3.3 PPTP Server Status

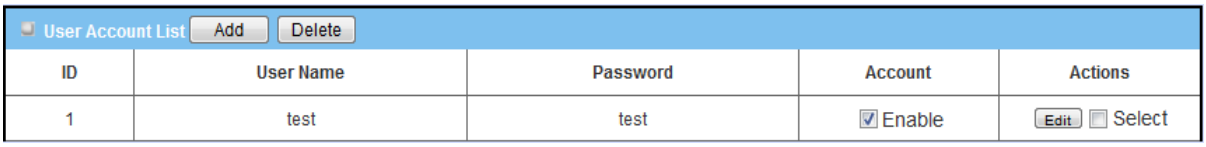
The user name and connection information for each connected PPTP client to the PPTP server of the Business Security Gateway will be shown in this table.



1. **Refresh:** To refresh the PPTP Server Status each 2 seconds by clicking on the "Refresh" button.
2. **Disconnect:** To terminate the connection between PPTP server and remote dialing in PPTP clients by clicking on the "Disconnect" button.

3.2.3.3.4 User Account List

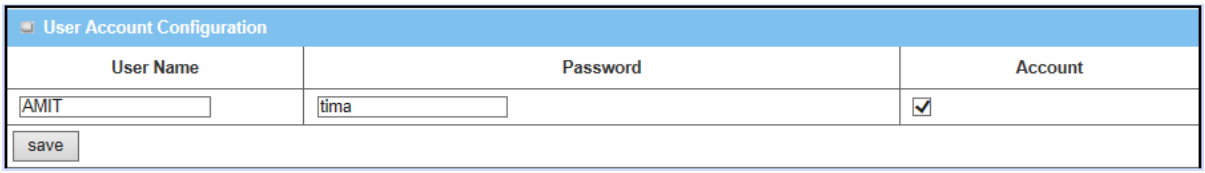
You can input up to 10 different user accounts for dialing in PPTP server.



1. **Add:** You can add one new user account by clicking on the "Add" button.
2. **Delete:** Delete selected user accounts by checking the "Select" box at the end of each user account list and then clicking on the "Delete" button.
3. **Account:** Check the "Enable" box to validate the user account.
4. **Edit:** You can edit one user account configuration by clicking on the "Edit" button at the end of each user account list.

3.2.3.3.5 User Account Configuration

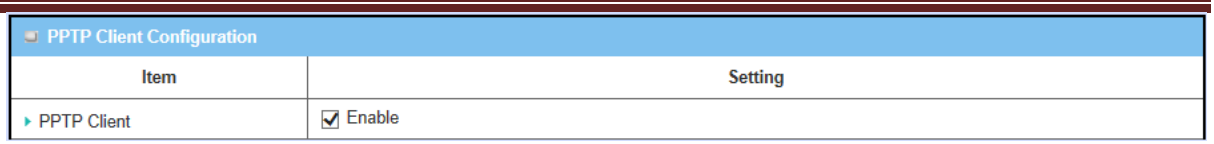
Add or edit one user account will activate the "User Account Configuration" screen.



1. **User Name:** Enter the user name of user account.
2. **Password:** Enter the password of user account.
3. **Account:** Check the "Enable" box to validate the user account.
4. **Save:** To save the user account configuration.

3.2.3.3.6 PPTP Client

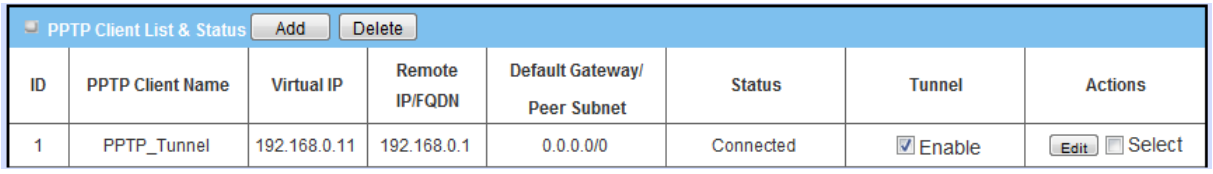
The Business Security Gateway also can behave as a PPTP client except PPTP server, and PPTP client tries to establish a PPTP tunnel to remote PPTP server. All client hosts in the Intranet of Business Security Gateway can access LAN servers behind the PPTP server.



1. **PPTP Client:** Enable or disable PPTP client function.

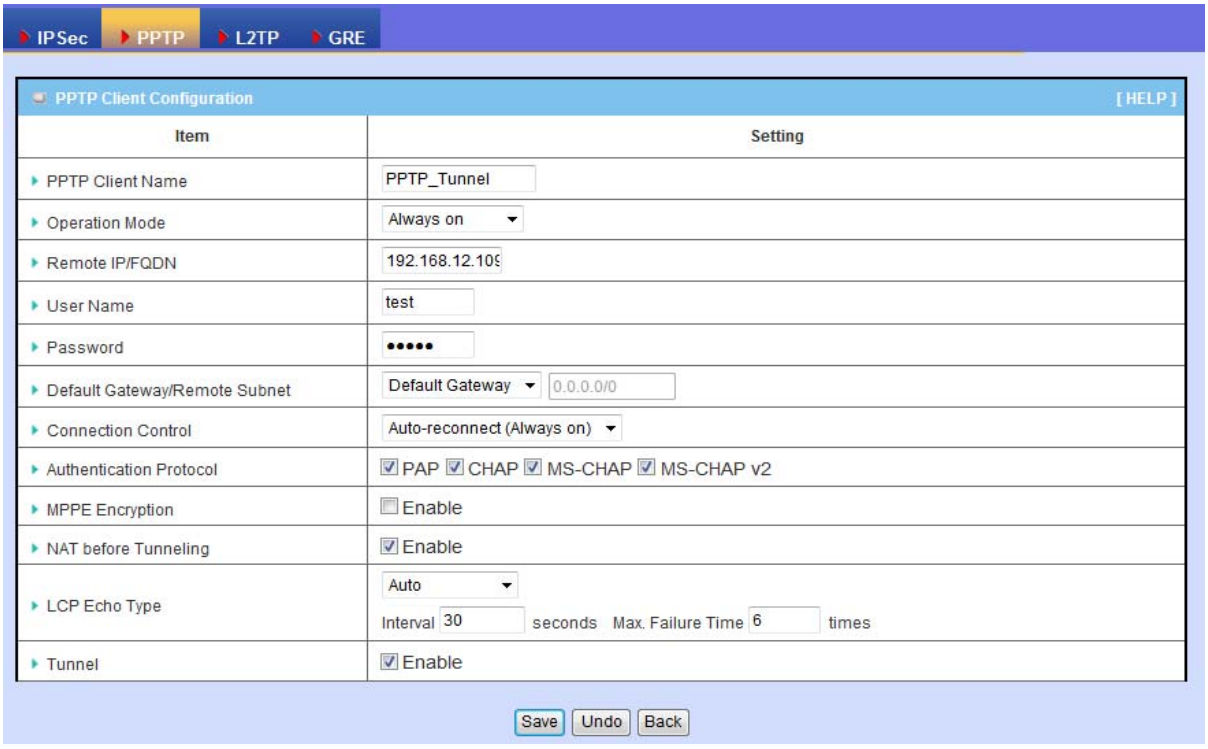
3.2.3.3.7 PPTP Client List & Status

You can add new up to 22 different PPTP client tunnels by clicking on the “Add” button, and modify each tunnel configuration by clicking on the corresponding “Edit” button at the end of each existed tunnel.



1. **Add:** You can add one new PPTP client tunnel by clicking on the “Add” button.
2. **Delete:** Delete selected tunnels by checking the “Select” box at the end of each tunnel list and then clicking on the “Delete” button.
3. **Tunnel:** Check the “Enable” box to activate the tunnel.
4. **Edit:** You can edit one PPTP client tunnel configuration by clicking on the “Edit” button at the end of each tunnel list.

3.2.3.3.8 PPTP Client Configuration



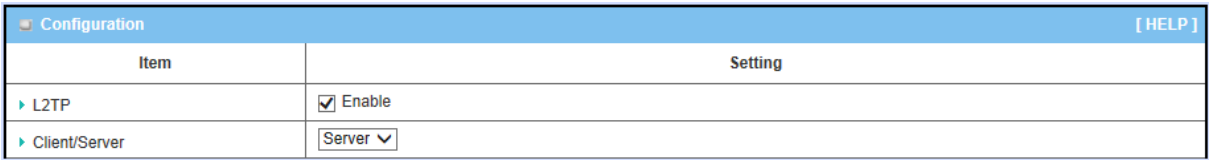
1. **PPTP Client Name:** The name of this tunnel.
2. **Operation Mode:** Default is “Always on” and other options depend on product models.

3. **Peer IP/Domain:** The IP address or Domain name of remote PPTP server.
4. **User Name:** The user name which can be validated by remote PPTP server.
5. **Password:** The password which can be validated by remote PPTP server.
6. **Default Gateway/Peer Subnet:** You can choose “Default Gateway” option or “Peer Subnet” option here. When “Default Gateway” is chosen, all traffic from Intranet of Business Security Gateway goes over this PPTP tunnel if these packets don’t match the Peer Subnet of other PPTP tunnels. There is only one PPTP tunnel to own the “Default Gateway” property. However, when “Peer Subnet” is chosen, peer subnet parameter needs to be filled and it should be the LAN subnet of remote PPTP server. If an Intranet packet wants to go to this peer subnet, the PPTP tunnel will be established automatically.
7. **Connection Control:** There are three connection control options for users to choose when the PPTP tunnel is established. You can choose “Connect-on-Demand”, “Auto Reconnect (always-on)”, or “Manually”. By default, it is “Auto Reconnect (always-on)”.
8. **Authentication Protocol:** You can choose authentication protocol as PAP, CHAP, MS-CHAP, or MS-CHAP v2. The protocol you choose must be supported by remote PPTP server.
9. **MPPE Encryption:** Check the “Enable” box to activate MPPE encryption. Please note that MPPE needs to work with MS-CHAP or MS-CHAP v2 authentication methods.
10. **NAT before Tunneling**: Check the “Enable” box to let hosts in the Intranet of Business Security Gateway can go to access Internet via remote PPTP server. By default, it is enabled. However, if you want the remote PPTP Server to monitor the Intranet of local Business Security Gateway, the option can’t be enabled.
11. **LCP Echo Type:** Choose the way to do connection keep alive. By default, it is “Auto” option that means system will automatically decide the time interval between two LCP echo requests and the times that system can retry once system LCP echo fails. You also can choose “User-defined” option to define the time interval and the retry times by yourself. The last option is “Disable”.
12. **Tunnel**: Check the “Enable” box to activate the tunnel.

3.2.3.4 L2TP

In computer networking, Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs. It does not provide any encryption or confidentiality by itself. Rather, it relies on an encryption protocol that it passes within the tunnel to provide privacy.

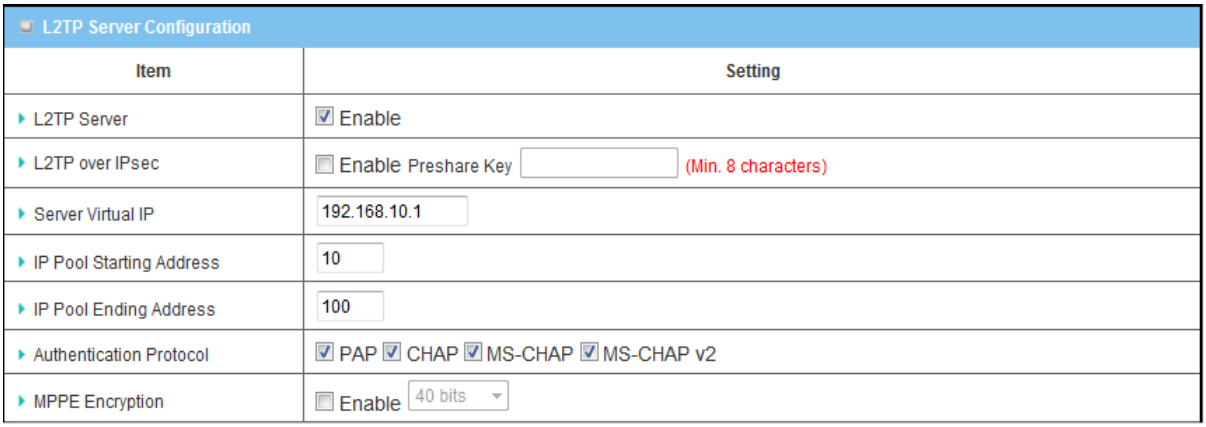
The Business Security Gateway can behave as a L2TP server and a L2TP client at the same time.



1. **L2TP:** Check the “Enable” box to activate L2TP client and server functions.
2. **Client/Server:** Choose Server or Client to configure corresponding role of L2TP VPN tunnels for the Business Security Gateway beneath the choosing screen.

3.2.3.4.1 L2TP Server Configuration

The Business Security Gateway can behave as a L2TP server, and it allows remote hosts to access LAN servers behind the L2TP server. The device can support four authentication methods: PAP, CHAP, MS-CHAP and MS-CHAP v2. Users can also enable MPPE encryption when using MS-CHAP or MS-CHAP v2.

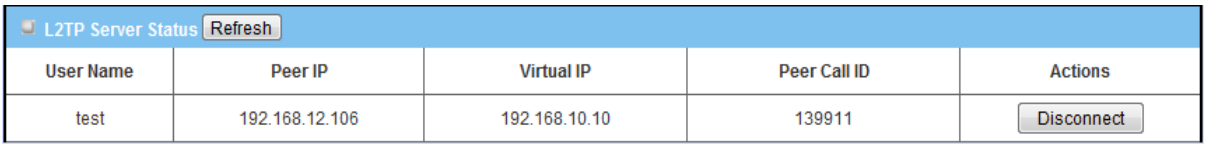


1. **L2TP Server:** Enable or disable L2TP server function.
2. **L2TP over IPSec:** L2TP over IPSec VPNs allow you to transport data over the Internet, while still maintaining a high level of security to protect data. Enter a Pre-shared key that system will use it in IPSec tunneling. And when you use some devices, like Apple related mobile devices, you should also know that key to establish L2TP over IPSec tunnels.
3. **Server Virtual IP:** It is the virtual IP address of L2TP server used in L2TP tunneling. This IP address should be different from the gateway one and members of LAN subnet of Business Security Gateway.
4. **IP Pool Starting Address:** This device will assign an IP address for each remote L2TP client. This value indicates the beginning of IP pool.
5. **IP Pool Ending Address:** This device will assign an IP address for each remote L2TP client. This value indicates the end of IP pool.
6. **Authentication Protocol:** You can choose authentication protocol as PAP, CHAP, MS-CHAP, or MS-CHAP v2.

7. **MPPE Encryption:** Check the “Enable” box to activate MPPE encryption. Please note that MPPE needs to work with MS-CHAP or MS-CHAP v2 authentication method. In the meantime, you also can choose encryption length of MPPE encryption, 40 bits, 56 bits or 128 bits.

3.2.3.4.2 L2TP Server Status

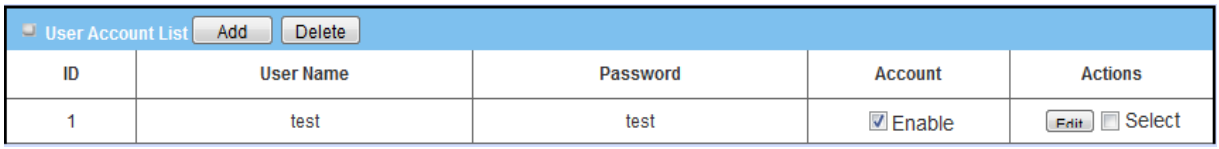
The user name and connection information for each connected L2TP client to the L2TP server of the Business Security Gateway will be shown in this table.



1. **Refresh:** To refresh the L2TP Server Status each 2 seconds by clicking on the “Refresh” button.
2. **Disconnect:** To terminate the connection between L2TP server and remote dialing in L2TP clients by clicking on the “Disconnect” button.

3.2.3.4.3 User Account List

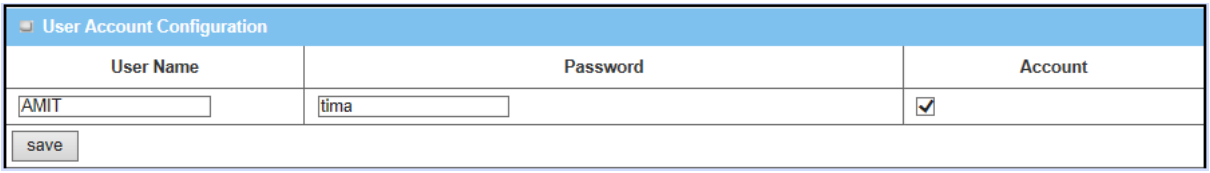
You can input up to 10 different user accounts for dialing in L2TP server.



1. **Add:** You can add one new user account by clicking on the “Add” button.
2. **Delete:** Delete selected user accounts by checking the “Select” box at the end of each user account list and then clicking on the “Delete” button.
3. **Account:** Check the “Enable” box to validate the user account.
4. **Edit:** You can edit one user account configuration by clicking on the “Edit” button at the end of each user account list.

3.2.3.4.4 User Account Configuration

Add or edit one user account will activate the “User Account Configuration” screen.



1. **User Name:** Enter the user name of user account.
2. **Password:** Enter the password of user account.
3. **Account:** Check the “Enable” box to validate the user account.
4. **Save:** To save the user account configuration.

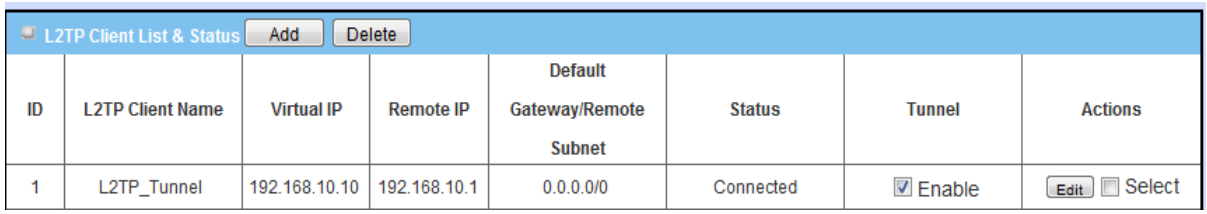
3.2.3.4.5 L2TP Client

The Business Security Gateway also can behave as a L2TP client except L2TP server, and L2TP client tries to establish a L2TP tunnel to remote L2TP server. All client hosts in the Intranet of Business Security Gateway can access LAN servers behind the L2TP server.

1. **L2TP Client Configuration:** Enable or disable L2TP client function.

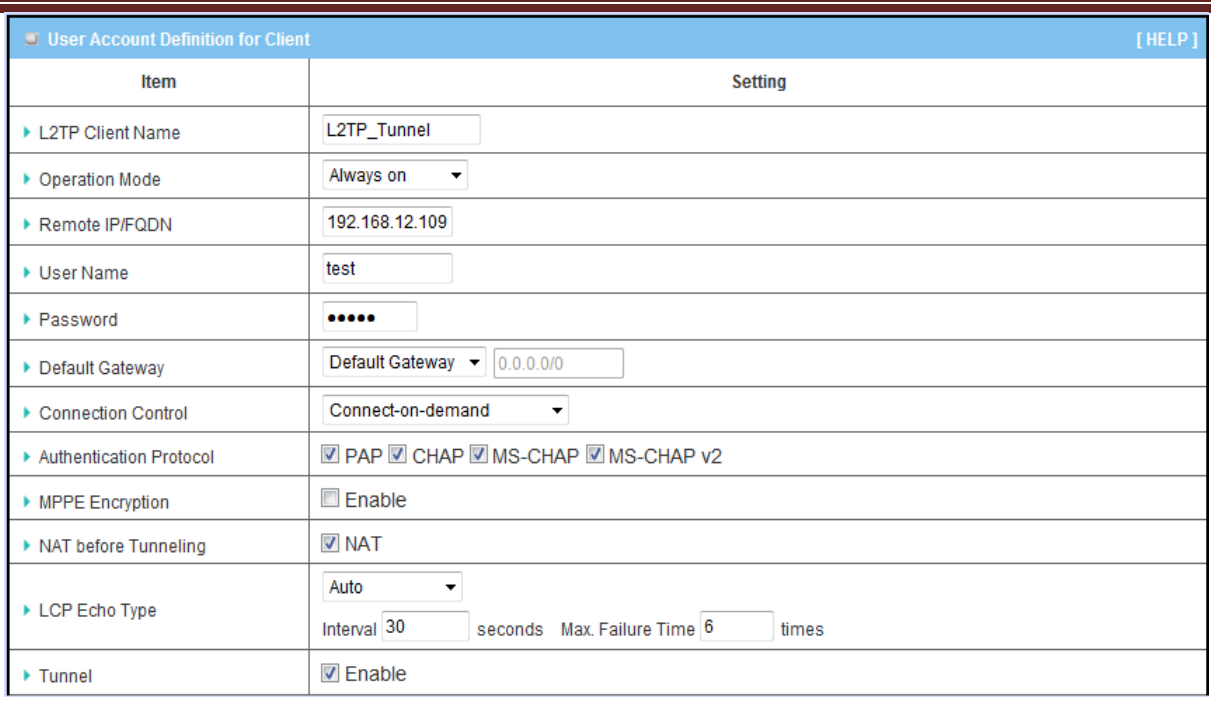
3.2.3.4.6 L2TP Client List & Status

You can add new up to 22 different L2TP client tunnels by clicking on the “Add” button, and modify each tunnel configuration by clicking on the corresponding “Edit” button at the end of each existed tunnel.



1. **Add:** You can add one new L2TP client tunnel by clicking on the “Add” button.
2. **Delete:** Delete selected tunnels by checking the “Select” box at the end of each tunnel list and then clicking on the “Delete” button.
3. **Tunnel:** Check the “Enable” box to activate the tunnel.
4. **Edit:** You can edit oneL2TPTP client tunnel configuration by clicking on the “Edit” button at the end of each tunnel list.

3.2.3.4.7 L2TP Client Configuration



1. **L2TP Client Name:** The name of this tunnel.
2. **Operation Mode:** Default is “Always on” and other options depend on product models.
3. **Peer IP/Domain:** The IP address or Domain name of remote L2TP server.
4. **User Name:** The user name which can be validated by remote L2TP server.
5. **Password:** The password which can be validated by remote L2TP server.
6. **Default Gateway/Peer Subnet:** You can choose “Default Gateway” option or “Peer Subnet” option here. When “Default Gateway” is chosen, all traffic from Intranet of Business Security Gateway goes over this L2TP tunnel if these packets don’t match the Peer Subnet of other L2TP tunnels. There is only one L2TP tunnel to own the “Default Gateway” property. However, when “Peer Subnet” is chosen, peer subnet parameter needs to be filled and it should be the LAN subnet of remote L2TP server. If an Intranet packet wants to go to this peer subnet, the L2TP tunnel will be established automatically.
7. **Connection Control:** There are three connection control options for users to choose when the L2TP tunnel is established. You can choose “Connect-on-Demand”, “Auto Reconnect (always-on)”, or “Manually”. By default, it is “Auto Reconnect (always-on)”.
8. **Authentication Protocol:** You can choose authentication protocol as PAP, CHAP, MS-CHAP, or MS-CHAP v2. The protocol you choose must be supported by remote L2TP server.
9. **MPPE Encryption:** Check the “Enable” box to activate MPPE encryption. Please note that MPPE needs to work with MS-CHAP or MS-CHAP v2 authentication methods.
10. **NAT before Tunneling**: Check the “Enable” box to let hosts in the Intranet of

Business Security Gateway can go to access Internet via remote PPTP server. By default, it is enabled. However, if you want the remote PPTP Server to monitor the Intranet of local Business Security Gateway, the option can't be enabled.

11. **LCP Echo Type:** Choose the way to do connection keep alive. By default, it is "Auto" option that means system will automatically decide the time interval between two LCP echo requests and the times that system can retry once system LCP echo fails. You also can choose "User-defined" option to define the time interval and the retry times by yourself. The last option is "Disable".
12. **Tunnel:** Check the "Enable" box to activate the tunnel.

3.2.3.5 GRE

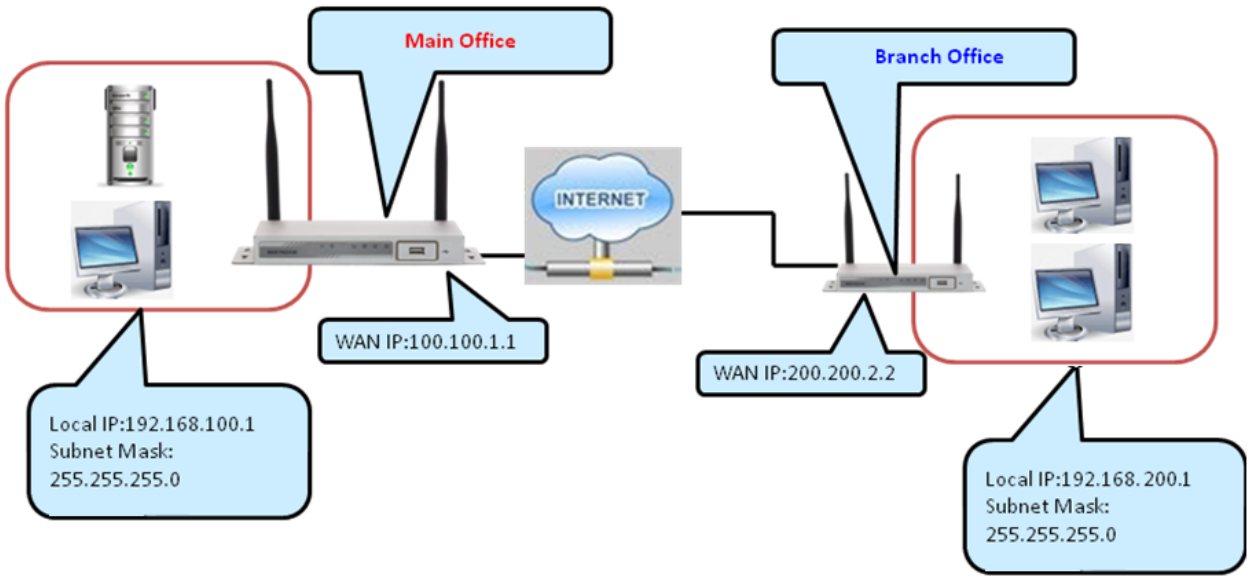
Generic Routing Encapsulation (GRE) is a tunneling protocol developed by Cisco Systems that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol internetwork.

3.2.3.5.1 GRE VPN Tunnel Scenario

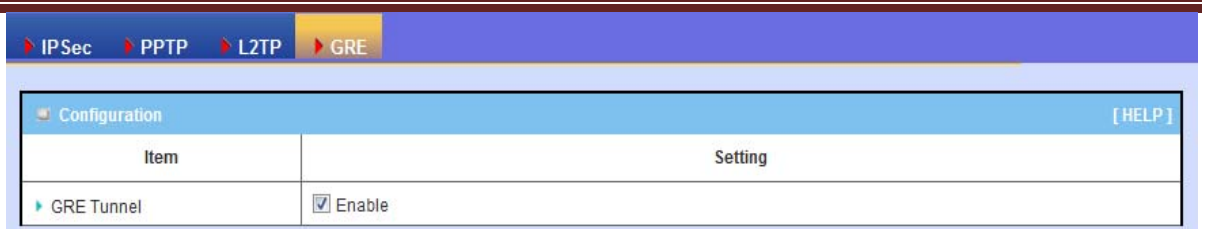
There is one common GRE VPN connection scenario as follows:

- GRE Server / Client Application

  The Business Security Gateway acts as GRE Server or Client role in SMB Headquarters or Branch Office.

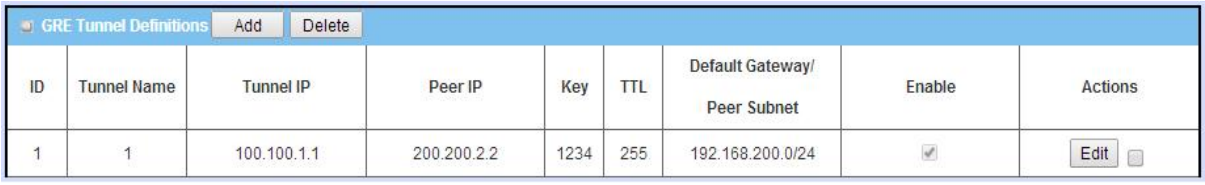


3.2.3.5.2 GRE Configuration



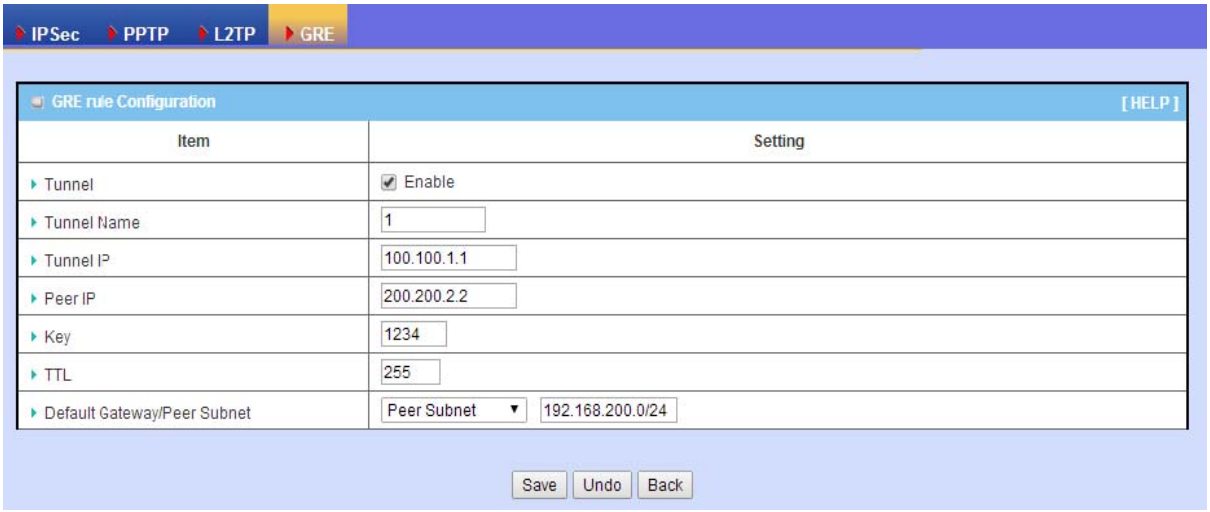
1. **GRE Tunnel:** Check the “Enable” box to activate the GRE tunnel function.

3.2.3.5.3 GRE Tunnel Definitions



1. **Add:** You can add one new GRE tunnel by clicking on the “Add” button.
2. **Delete:** Delete selected tunnels by checking the “Select” box at the end of each tunnel list and then clicking on the “Delete” button.
3. **Tunnel:** Check the “Enable” box to activate the GRE tunnel.
4. **Edit:** You can edit one tunnel configuration by clicking the “Edit” button at the end of each tunnel list.

3.2.3.5.4 GRE rule Configuration



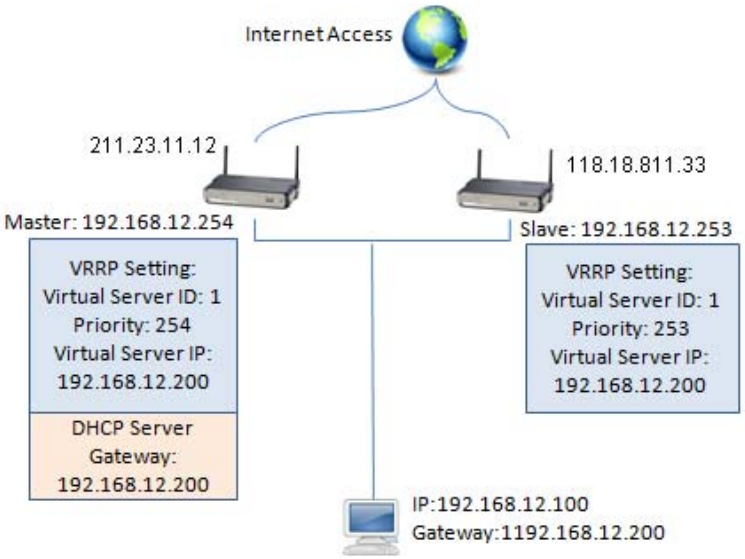
1. **Tunnel:** Enable or disable this GRE tunnel.
2. **Tunnel Name:** The name of this GRE tunnel.
3. **Tunnel IP:** The gateway IP address of Business Security Gateway.
4. **Peer IP:** Enter the IP address of remote peer that you want to connect.
5. **Key:** Enter the password to establish GRE tunnel with remote host.
6. **TTL:** Time-To-Live for packets. The value is within 1 to 255. If a packet passes number of TTL routers and still can't reach the destination, then this packet will be dropped.
7. **Default Gateway/Peer Subnet:** You can choose “Default Gateway” option or

"Peer Subnet" option here. When "Default Gateway" is chosen, all traffic from Intranet of Business Security Gateway goes over this GRE tunnel if these packets don't match the Peer Subnet of other GRE tunnels. There is only one GRE tunnel to own the "Default Gateway" property. However, when "Peer Subnet" is chosen, peer subnet parameter needs to be filled and it should be the LAN subnet of remote GRE server. If an Intranet packet wants to go to this peer subnet, the GRE tunnel will be established automatically.

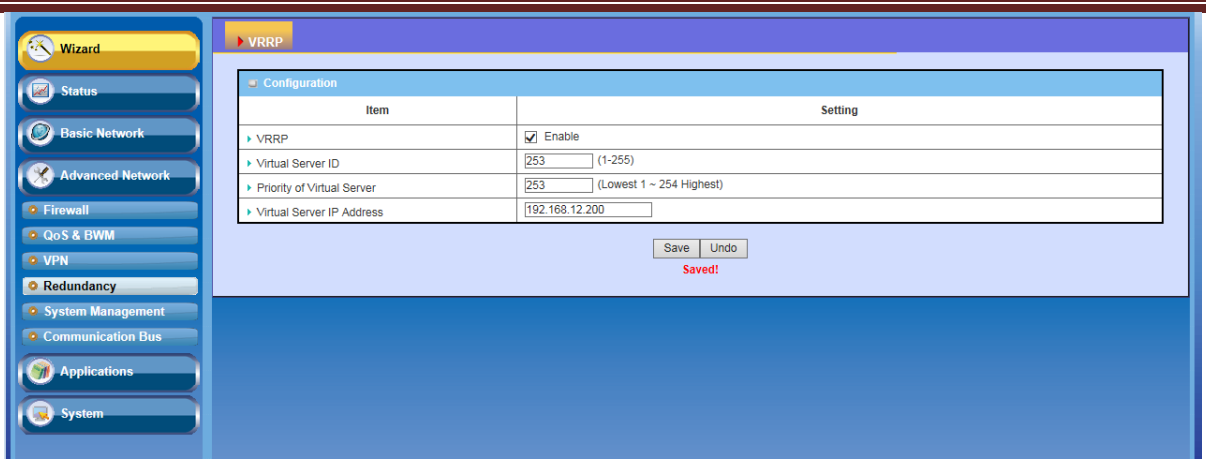
3.2.4 Redundancy

3.2.4.1 VRRP

The Virtual Router Redundancy Protocol (VRRP) is a computer networking protocol providing device redundancy. It allows a backup router or switch to automatically take over if the primary (master) router or switch fails. This increases the availability and reliability of routing paths via automatic default gateway selections on an IP network.



The protocol achieves this by creation of virtual routers, which are an abstract representation of multiple routers, i.e. master and backup routers, acting as a group. The default gateway of a participating host is assigned to the virtual router instead of a physical router. If the physical router that is routing packets on behalf of the virtual router fails, another physical router is selected to automatically replace it. The physical router that is forwarding packets at any given time is called the master router.



1. **VRRP:** Enable or disable the VRRP function.
2. **Virtual Server ID**: Means Group ID. Specify the ID number of the virtual server. Its value ranges from 1 to 255.
3. **Priority of Virtual Server:** Specify the priority to use in VRRP negotiations. Valid values are from 1 to 254, and a larger value has higher priority.
4. **Virtual Server IP Address**: Specify the IP address of the virtual server.

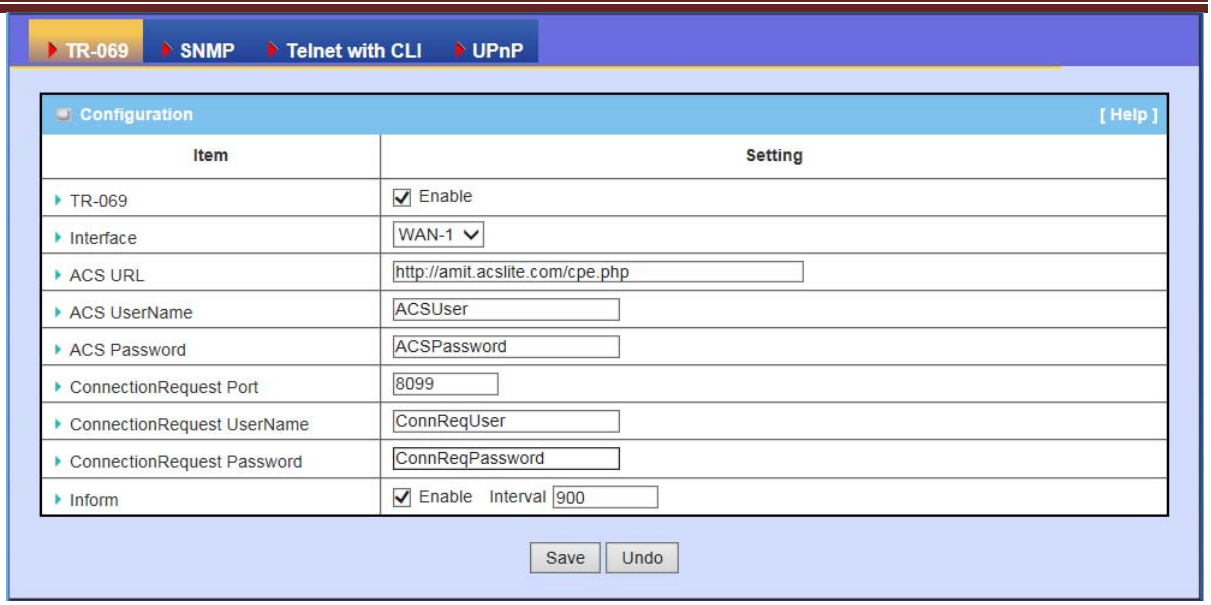
Click on “Save” to store what you just select or “Undo” to give up.

3.2.5 System Management

This device supports many system management protocols, such as TR-069, SNMP, Telnet with CLI and UPnP. You can finish those configurations in this sub-section.

3.2.5.1 TR-069

TR-069 (Technical Report 069) is a Broadband Forum technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices, like this gateway device. As a bidirectional SOAP/HTTP-based protocol, it provides the communication between customer-premises equipment (CPE) and Auto Configuration Servers (ACS). The Security Gateway is such CPE.



TR-069 is a customized feature for ISP; it is not recommend that you change the configuration for this. If you have any problem in using this feature for device management, please contact with your ISP or the ACS provider for help. At the right upper corner of TR-069 Setting screen, one “[Help]” command let you see the same message about that.

3.2.5.2 SNMP

In brief, SNMP, the Simple Network Management Protocol, is a protocol designed to give a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.

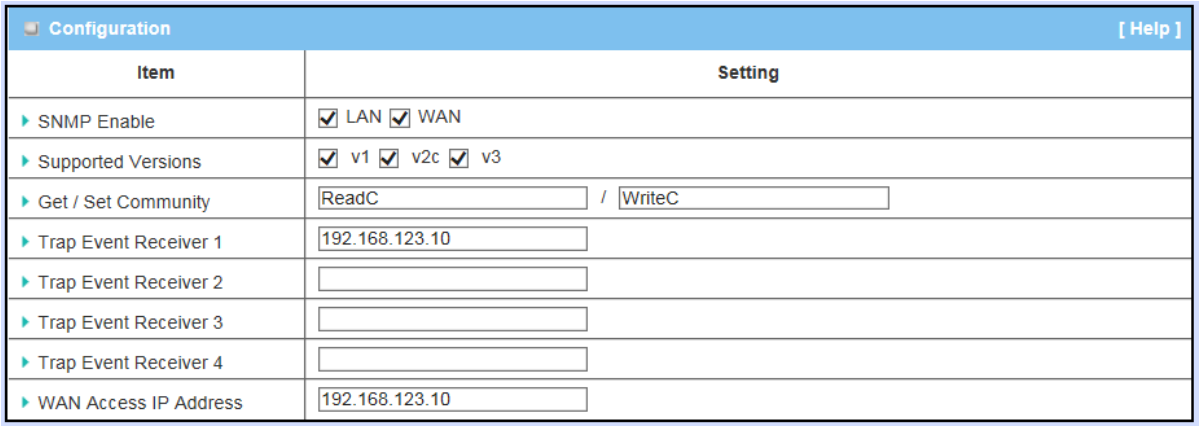
In typical SNMP uses, one or more administrative computers, called managers, have the task of monitoring or managing a group of hosts or devices on a computer network. Each managed system executes, at all times, a software component called an agent which reports information via SNMP to the manager.

SNMP agents expose management data on the managed systems as variables. The protocol also permits active management tasks, such as modifying and applying a new configuration through remote modification of these variables. The variables accessible via SNMP are organized in hierarchies. These hierarchies, and other metadata (such as type and description of the variable), are described by Management Information Bases (MIBs).

The device supports several public MIBs and one private MIB for the SNMP agent. The supported MIBs are as follow:

- Supported MIBs

- MIB-II (RFC 1213, Include IPv6)
- IF-MIB, IP-MIB, TCP-MIB, UDP-MIB
- SMIv1 and SMIv2
- SNMPv2-TM and SNMPv2-MIB
- AMIB (Proroute Private MIB)



1. **SNMP Enable**: You can check “Local (LAN)”, “Remote (WAN)” or both to enable SNMP function. If “Local (LAN)” is checked, this device will respond to the request from LAN. If “Remote (WAN)” is checked, this device will respond to be request from WAN.
2. **WAN Access IP Address:** If you want to limit the remote SNMP access to specific computer, please enter the PC`s IP address. The default value is 0.0.0.0, and it means that any internet connected computer can get some information of the device with SNMP protocol.
3. **SNMP Version:** Supports SNMP V1 and V2c.
4. **Get Community:** The community of GetRequest that this device will respond. This is a text password mechanism that is used to weakly authenticate queries to agents of managed network devices.
5. **Set Community:** The community of SetRequest that this device will accept.
6. **Trap Event Receiver 1 ~ 4:** Enter the IP addresses or Domain Name of your SNMP Management PCs. You have to specify it, so that the device can send SNMP Trap message to the management PCs consequently.
7. **WAN Access IP Address:** The IP address of remote control site to manage the device by using SNMP protocol.

A User Privacy table is used for only SNMP v3. It defines the user list and their privacy and authority settings.

User Privacy Definition

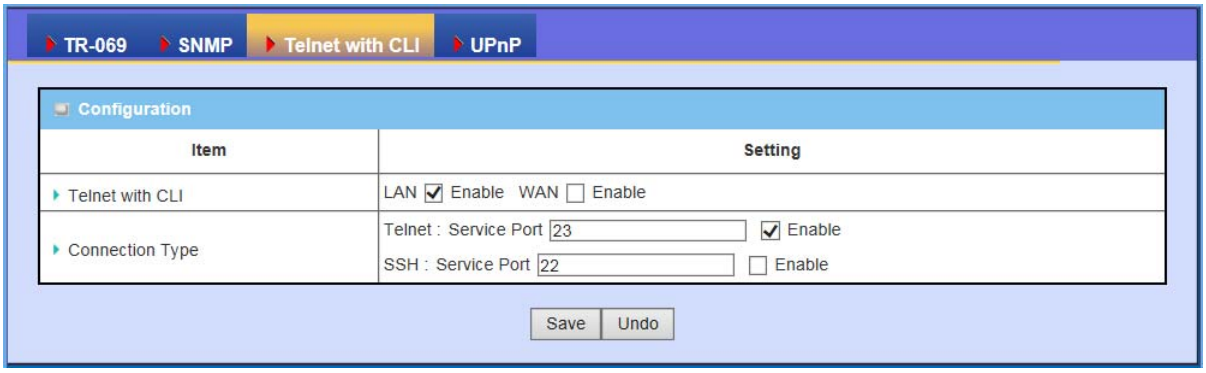
ID	User Name	Password	Authentication	Encryption	Privacy Mode	Privacy Key	Authority	Enable	Actions
1	User1	Password1	MD5	DES	authNoPriv		Read / Read/Write	☑	Edit
2	User2	Password2	MD5	DES	authPriv	1234567890	Read / Read/Write	☑	Edit
3	User3		MD5	DES	noAuthNoPriv		Read / Read/Write	☑	Edit
4			MD5	Disable	authNoPriv	Disable	Read	☐	Edit
5			MD5	Disable	authNoPriv	Disable	Read	☐	Edit

1. **User Name**: Input the name for a user.
2. **Password & Authentication**: Input the password for a user and choose the hashing algorithm for authentication. However, they will not be necessary when you choose the privacy mode to be "noAuthPriv" for the user account.
3. **Privacy Mode:** Choose the privacy mode for the specific user. There are three options, "NoAuthNoPriv", "AuthNoPriv" and "AuthPriv".
4. **Privacy Key & Encryption:** Input the privacy key for a user and choose the encryption algorithm for security.
5. **Authority:** Specify the Read or Write authority for the user account.
6. **Enable:** To activate the user account by checking the Enable box.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

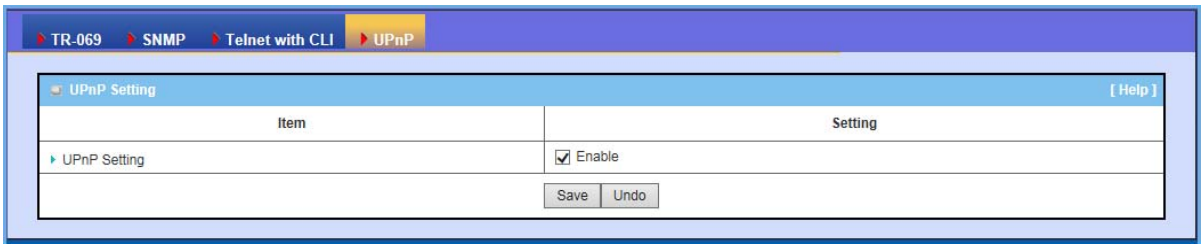
3.2.5.3 Telnet with CLI

A command-line interface (CLI), also known as command-line user interface, console user interface, and character user interface (CUI), is a means of interacting with a computer program where the user (or client) issues commands to the program in the form of successive lines of text (command lines). The interface is usually implemented with a command line shell, which is a program that accepts commands as text input and converts commands to appropriate operating system functions. Programs with command-line interfaces are generally easier to automate via scripting. The device supports both Telnet and SSH CLI with default service port 23 and 22, respectively. And it also accepts commands from both LAN and WAN sides.



3.2.5.4 UPnP

UPnP Internet Gateway Device (IGD) Standardized Device Control Protocol is a NAT port mapping protocol and is supported by some NAT routers. It is a common communication protocol of automatically configuring port forwarding. Applications using peer-to-peer networks, multiplayer gaming, and remote assistance programs need a way to communicate through home and business gateways. Without IGD one has to manually configure the gateway to allow traffic through, a process which is error prone and time consuming.



This device supports the UPnP Internet Gateway Device (IGD) feature. By default, it is disabled.

3.2.6 Certificate

In cryptography, a public key certificate (also known as a digital certificate or identity certificate) is an electronic document used to prove ownership of a public key. The certificate includes information about the key, information about its owner's identity, and the digital signature of an entity that has verified the certificate's contents are correct. If the signature is valid, and the person examining the certificate trusts the signer, then they know they can use that key to communicate with its owner[10].

10 Reference: http://en.wikipedia.org/wiki/Public_key_certificate.

In a typical public-key infrastructure (PKI) scheme, the signer is a certificate authority (CA), usually a company such as VeriSign which charges customers to issue certificates for them. In a web of trust scheme, the signer is either the key's owner (a self-signed certificate) or other users ("endorsements") whom the person examining the certificate might know and trust. The device also plays as a CA role.

Certificates are an important component of Transport Layer Security (TLS, sometimes called by its older name SSL), where they prevent an attacker from impersonating a secure website or other server. They are also used in other important applications, such as email encryption and code signing. Here, it can be used in IPSec tunneling for user authentication.

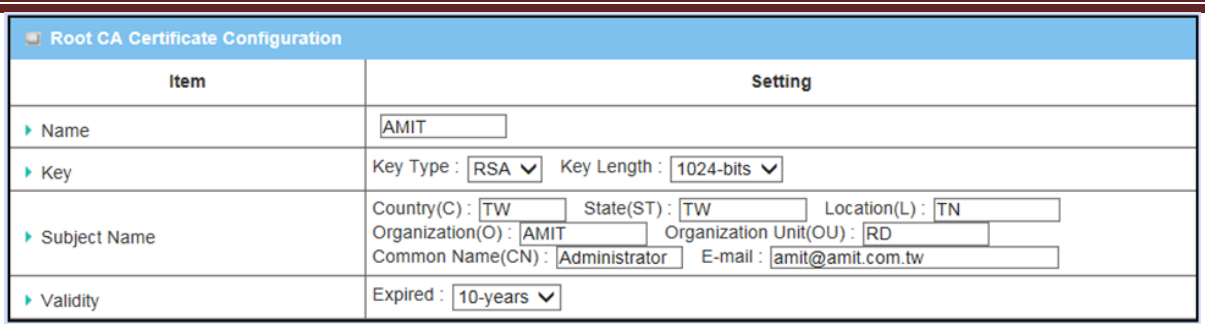
3.2.6.1 My Certificates

My Certificates include Root CA and Local Certificate List. Root CA is the top-most certificate of the tree, the private key of which is used to "sign" other certificates. Local Certificate is generated in this router. it can be self-signed by its Root CA or just generate a Certificate Signing Request (CSR) which can be signed by another external Root CA.

3.2.6.1.1 Root CA

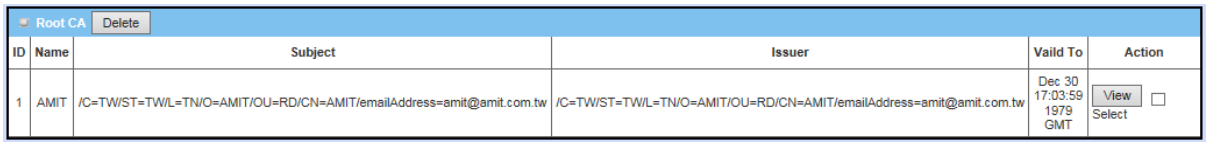
The device can serves as the Root CA. Root CA can sign local certificate when generate by selected self-signed or the Certificate Signing Request (CSR).

You can generate it by clicking on the "Generate" button.

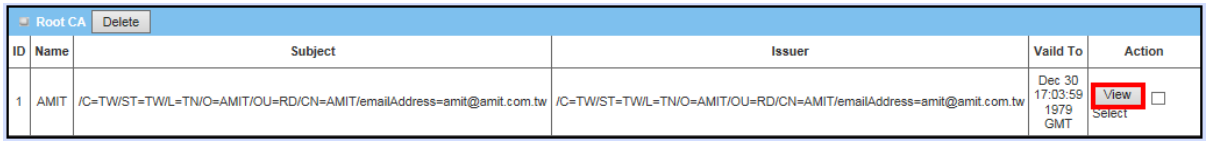


1. **Name:** Enter the name of root CA.
2. **Key:** Key Type is RSA. Key length: The size of the private key in bits. There are **five** key length can be selected: 512-bits, 765-bits, 1024-bits, 1536-bits, 2048-bits.
3. **Subject Name:** The Subject Name include seven information. Country(C): The two character country code of the certificate authority is located. State(ST): The state where the certificate authority is located. Location(L): The city where the certificate authority is located. Organization(O): The company whom the certificate authority belongs to. Organization Unit(OU): The company department whom the certificate authority belongs to. Common Name(CN): The common name for certificate authority. It's important as the common name for certificate authority. E-mail: The email address of a contact for the certificate authority.
4. **Validity:** The expiration date. There are four time period can be selected: 3-years, 5-years, 10-years, 20-years.

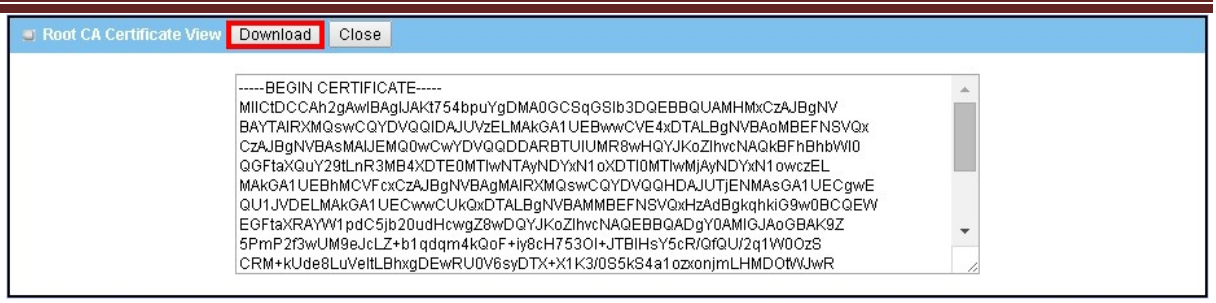
After successful generating the root CA, you also can delete it by checking the Select box and clicking on the "Delete" button.



You also can view its PEM codes by checking the "View" button.

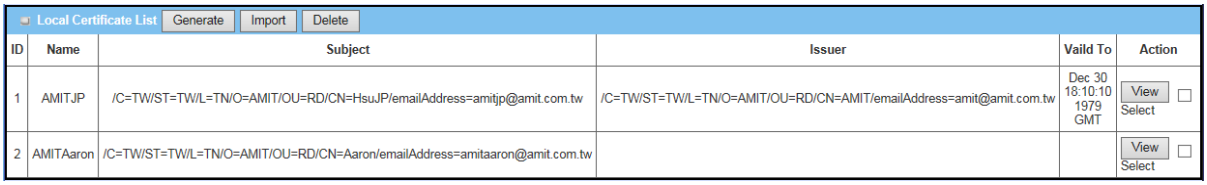


You can download the local certificate file by clicking on the "Download" button.

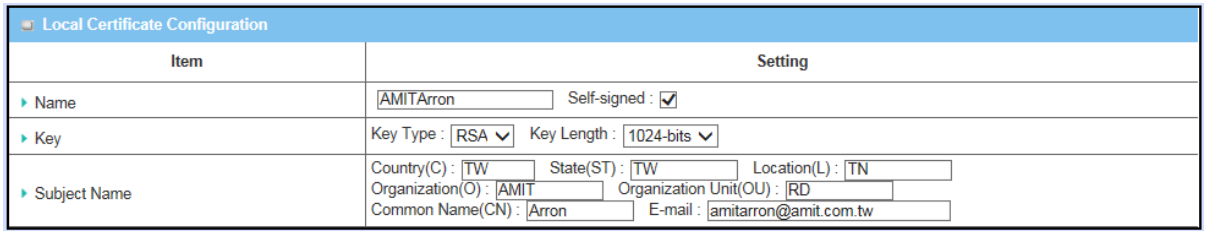


3.2.6.1.2 Local Certificate List

This feature can show the list of all certificates which contain information identifying the applicant. Each certificate involves field of the certificate name, subject, issuer and valid to.

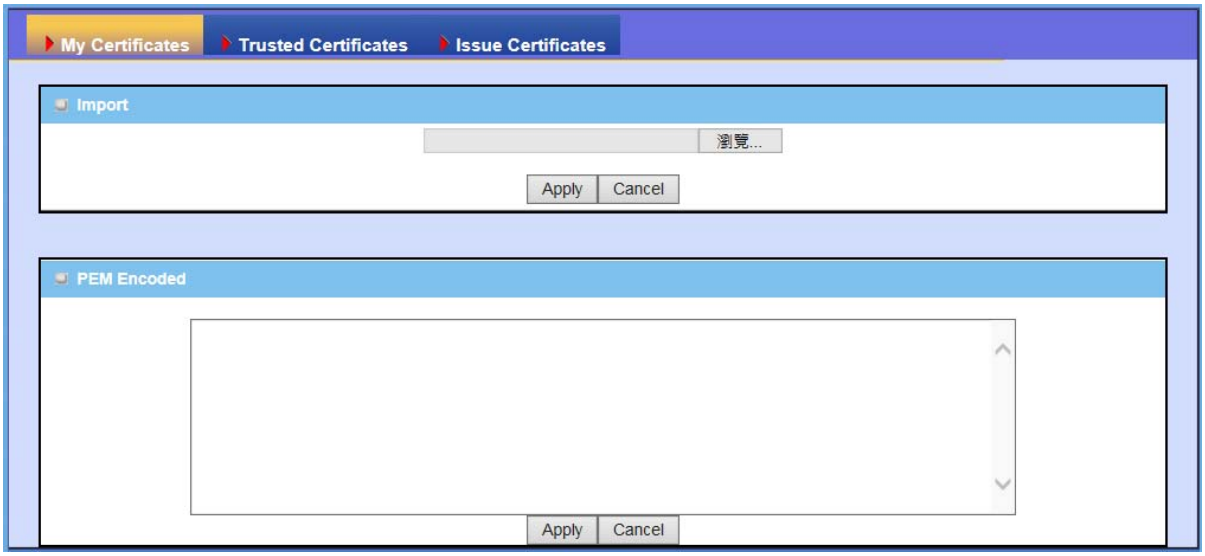


You can generate one certificate by clicking on the "Generate" button.

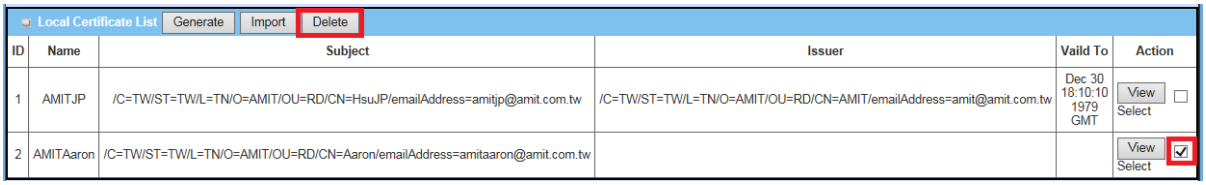


1. **Name:** Enter the name of certificate.
2. **Key:** Key Type is RSA. Key length: The size of the private key in bits. There are **five** key length can be selected: 512-bits, 765-bits, 1024-bits, 1536-bits, 2048-bits.
3. **Subject Name:** The Subject Name include seven information. Country(C): The two character country code of the certificate is located. State(ST): The state where the certificate is located. Location(L): The city where the certificate is located. Organization(O): The company whom the certificate belongs to. Organization Unit(OU): The company department whom the certificate belongs to. Common Name(CN): The common name for certificate. It's important as the common name for certificate. E-mail: The email address of a contact for the certificate.

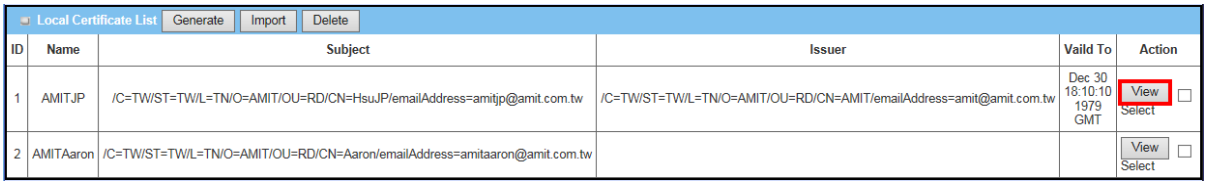
You also can import one certificate from your backup ones by clicking on the "Import" button. There are two approaches to import it. One is from a file and another is copy-paste the PEM codes in Web UI, and then click on the "Apply" button.



Certainly, you also can delete one local certificate by checking corresponding Select box and clicking on the "Delete" button.



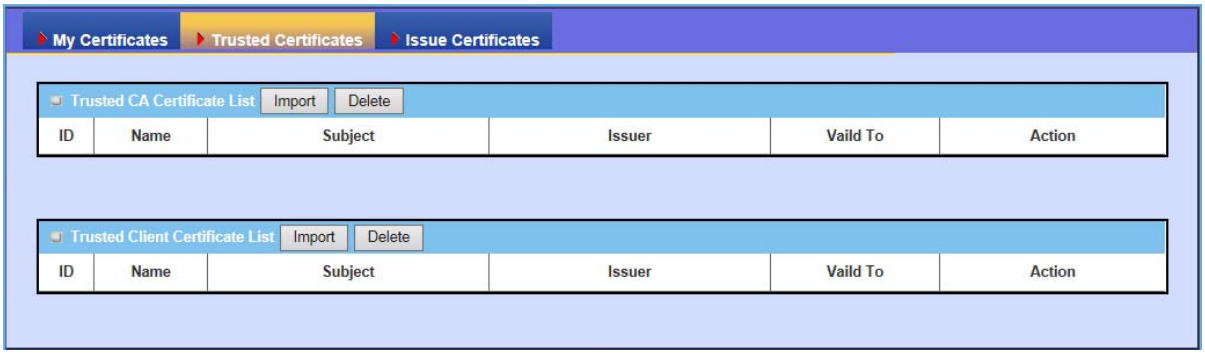
You can view its PEM codes by checking the "View" button.



You can download the local certificate file by clicking on the "Download" button.

3.2.6.2 Trusted Certificates

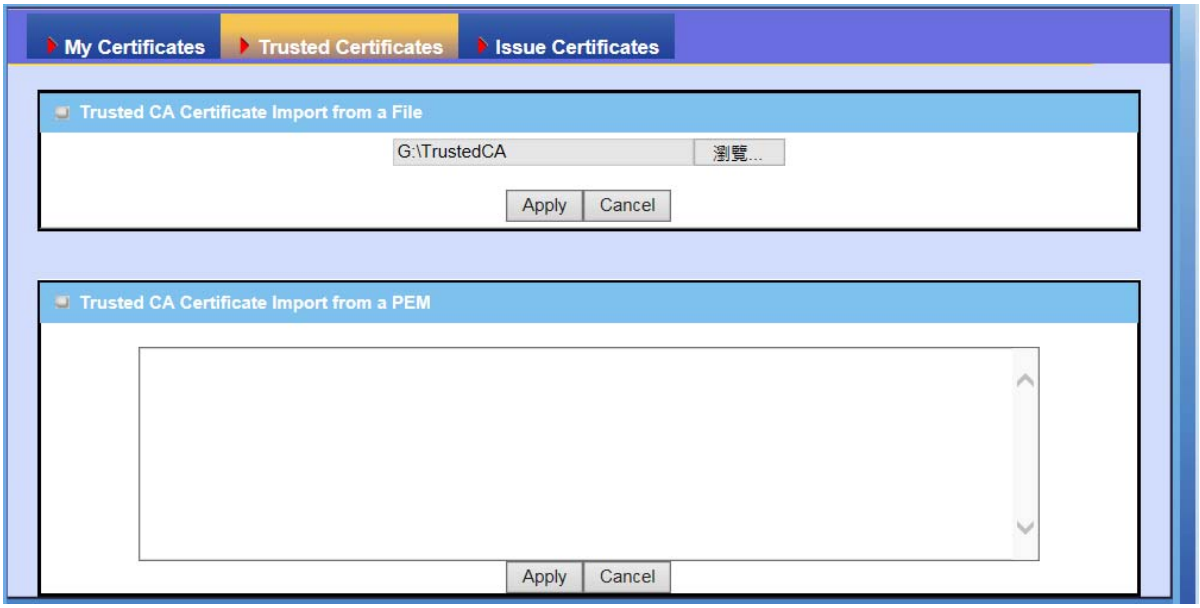
Trusted Certificates include Trusted CA Certificate List and Trusted Client Certificate List. The Trusted CA Certificate List which places the external trusted CA. The Trusted Client Certificate List which place the certificates what you trust.



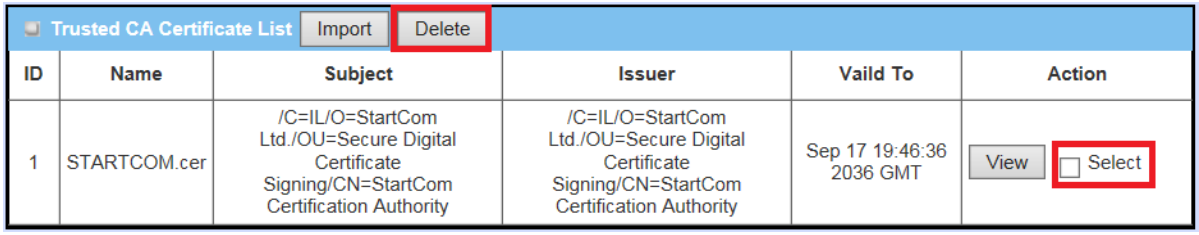
3.2.6.2.1 Trusted CA Certificate List

The device can let you import the certificate of trusted external CA by clicking on the "Import" button.

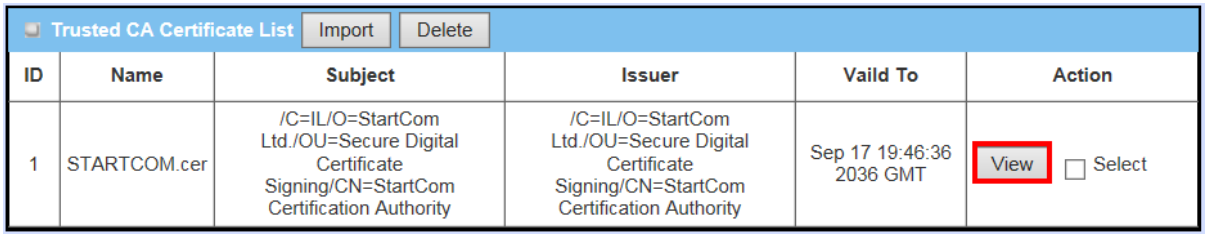
There are two approaches to import it. One is from a file and another is copy-paste the PEM codes in Web UI, and then click on the "Apply" button.



After successful importing the trusted external CA, you also can delete it by checking the Select box and clicking on the "Delete" button.



You can view its PEM codes by checking the "View" button.

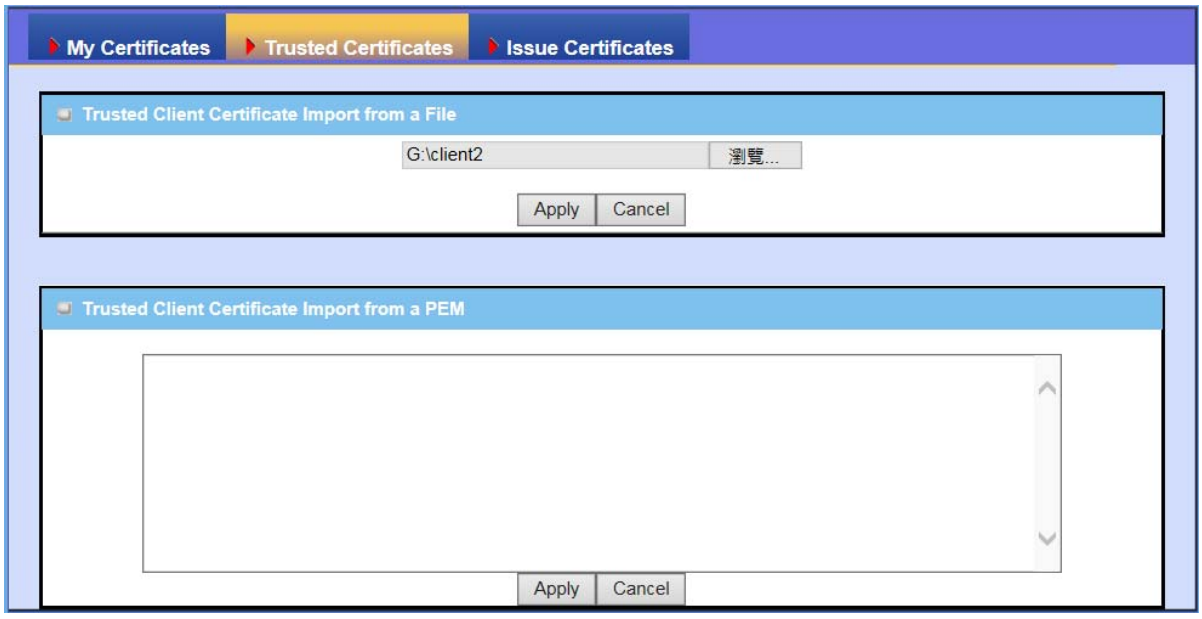


You can download the trusted CA file by clicking on the "Download" button.

3.2.6.2.2 Trusted Client Certificate List

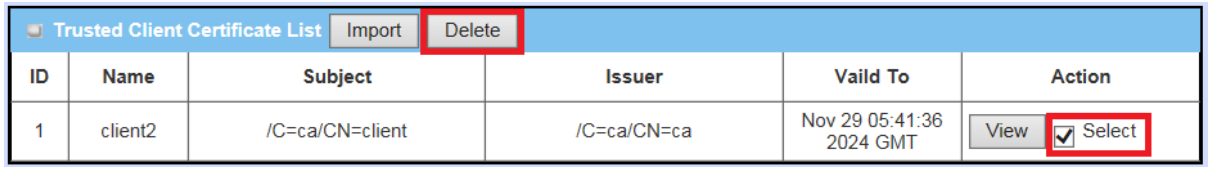
This feature can show the list of all certificates information. Each Certificate involve field of certificate name, subject, issuer and valid to.

You can import one trusted external client certificate by clicking on the "Import" button.

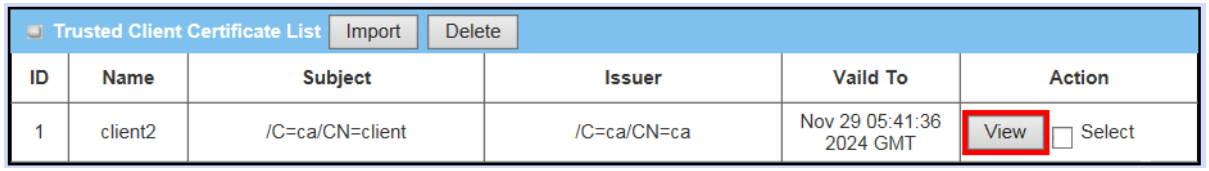


There are two approaches to import it. One is from a file and another is copy-paste the PEM codes in Web UI, and then click on the "Apply" button.

You also can delete one trusted client certificate by checking corresponding Select box and clicking on the "Delete" button.



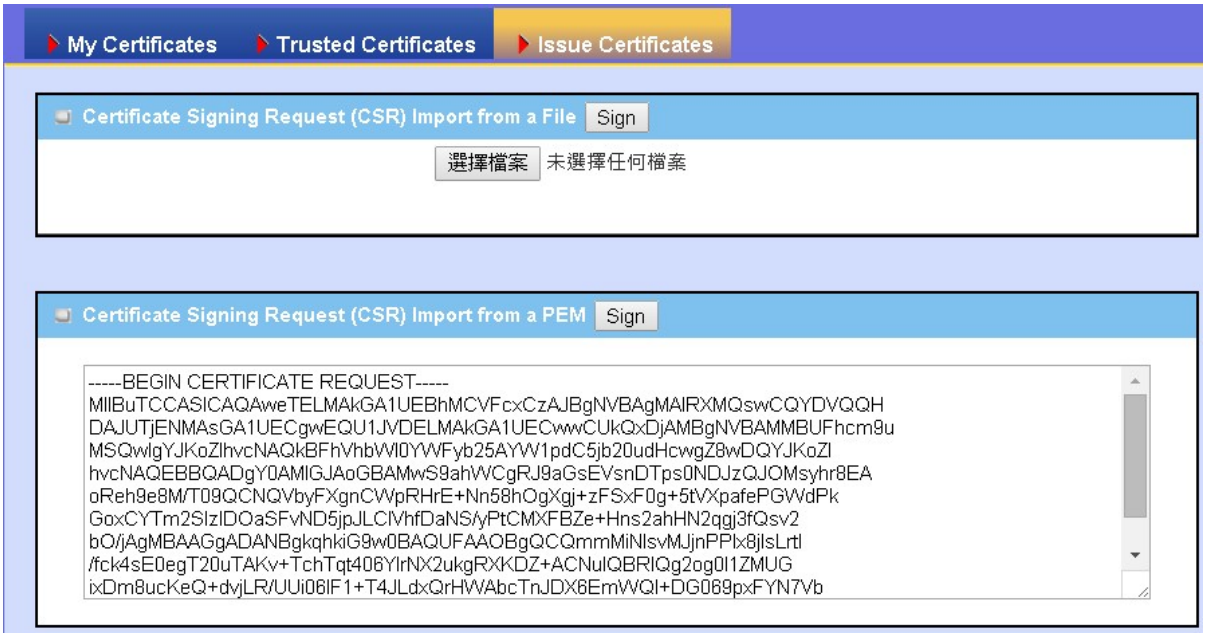
You can view its PEM codes by checking the "View" button.



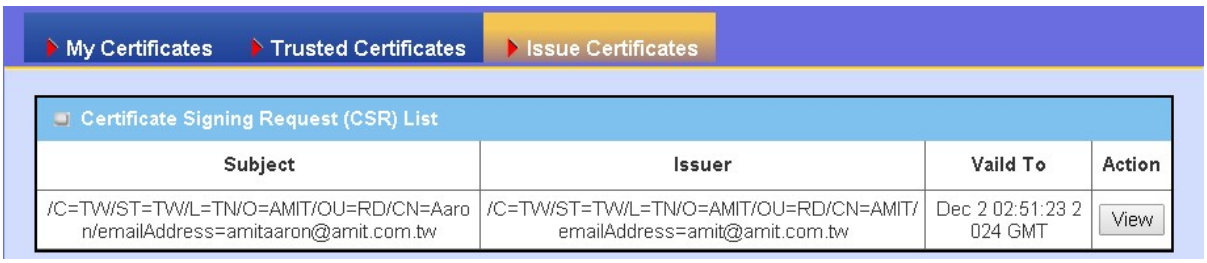
You can download the trusted client certificate file by clicking on the "Download" button.

3.2.6.3 Issue Certificates

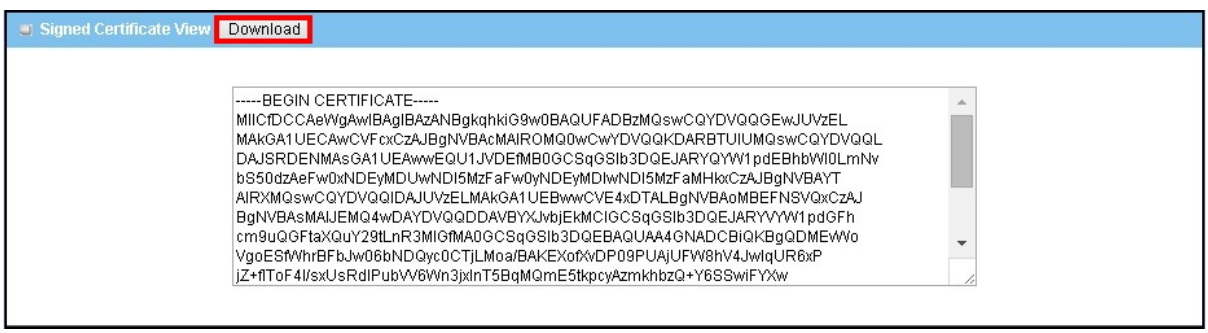
When you have a Certificate Signing Request (CSR) that needs to be certificated by the root CA of the device, you can issue the request here and let Root CA sign it. There are two approaches to issue it. One is from a file and another is copy-paste the CSR codes in Web UI, and then click on the "Sign" button.



After signing, the Issuer information can be show which is Root ca subject.



You also can view its PEM codes by checking the "View" button and download the issued certificate file by clicking on the "Download" button.



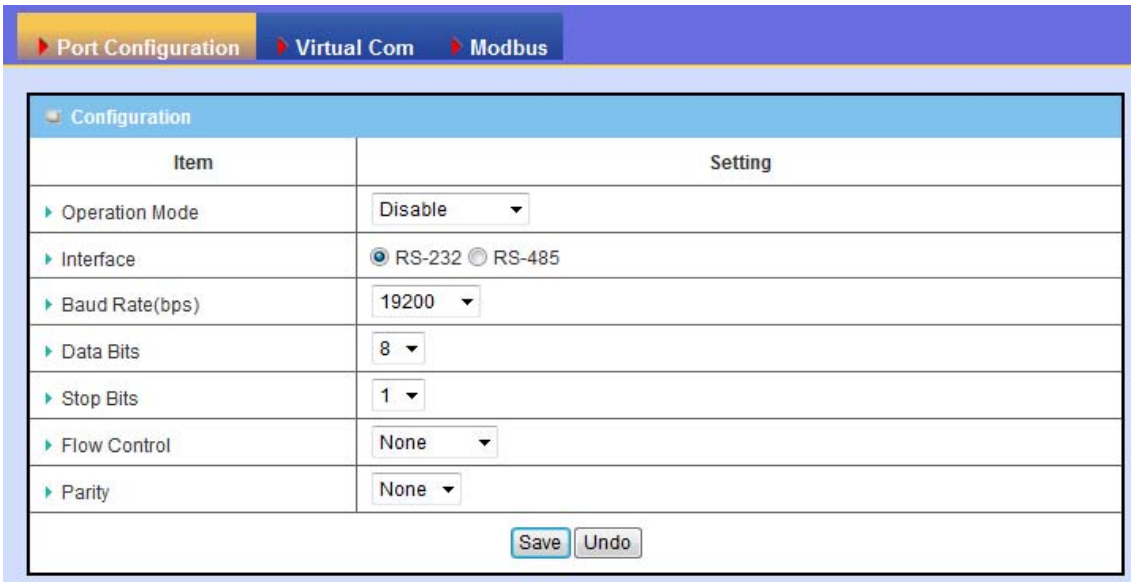
3.2.7 Communication Bus

The GEM-2M series provides the RJ12 female port for various serial communication use through connecting the RS-232 or RS-485 serial device to an IP-based Ethernet LAN. These communication protocols make user access serial devices anywhere over a local LAN or the Internet easily.

You can finish all related configurations of serial port in this section.

3.2.7.1 Port Configuration

Before using the function of Virtual COM or Modbus, you need to configure the RJ12 female port first.



1. **Operation Mode:** Choose the purpose of serial port. It can be “Virtual COM” or “Modbus”. You can also disable it to prevent anyone connects a unknown serial device to this gateway.
2. **Interface:** Choose RS-232 or RS-485.
3. **Baud Rate:** Set the baud rate (bps) of serial port. The value can be 9600, 19200, 38400, 57600, or 115200.
4. **Data Bits:** Choose 7 or 8 as the data bit.
5. **Stop Bits:** Choose 1 or 2 as the stop bit.
6. **Flow Control:** Choose RTS/CTS, DTS/DSR for flow control, or none.
7. **Parity:** Choose None, Even or Odd.

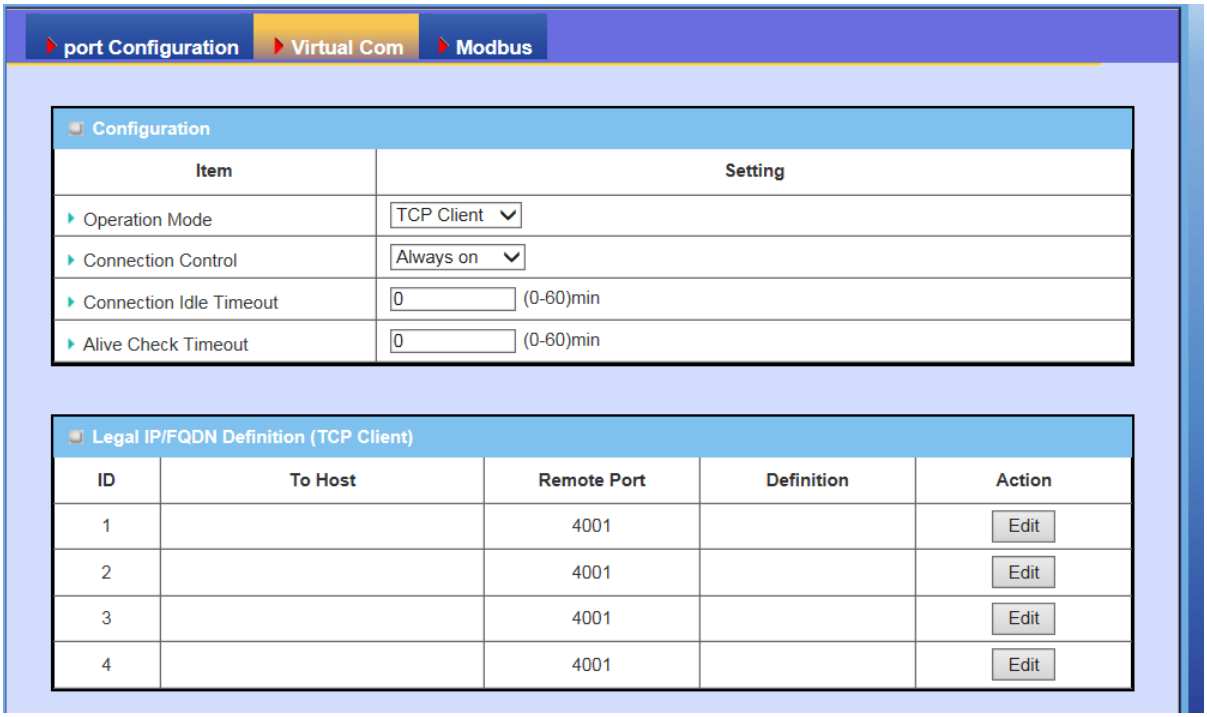
3.2.7.2 Virtual COM

Create a virtual COM port on user’s PC/Host and provide access to serial device

connected to serial port on GEMN-2M gateway. Therefore, users can access, control, and manage serial devices through Internet (fixed line, or cellular network) no matter where they are. There are four modes for virtual com connection: TCP Client, TCP Server, UDP, and RFC2217.

TCP Client Mode

In TCP Client mode, GEM-2M can actively establish a TCP connection to a pre-defined host computer when serial data arrives. After the data has been transferred, GEM-2M can automatically disconnect from the host computer by using the TCP alive check timeout or idle timeout settings.

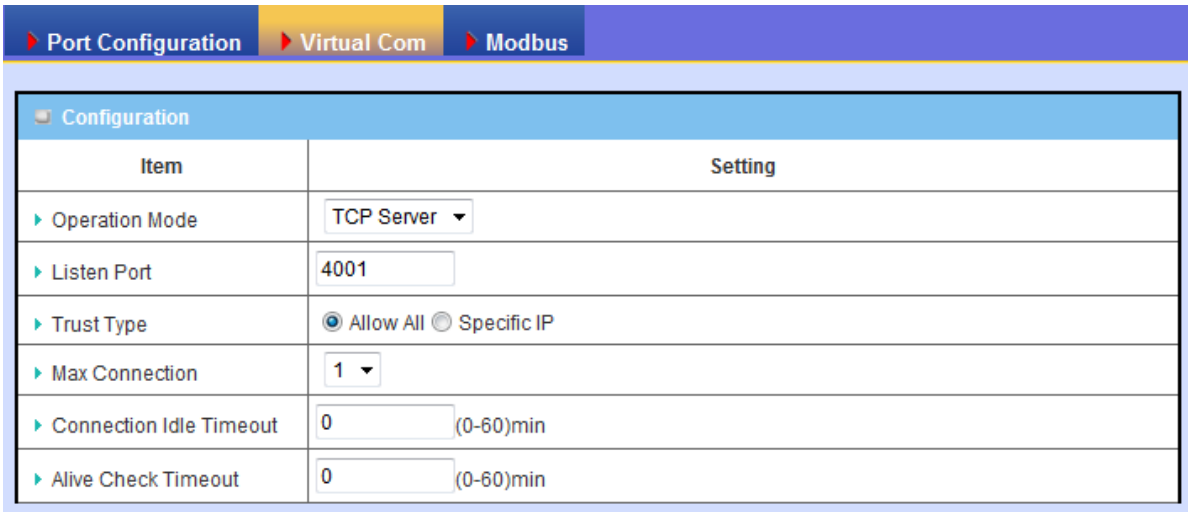


1. **Operation Mode:** Choose TCP Client.
2. **Connection Control:** Choose “Always on” if you want to keep TCP connection with TCP server all the time. Otherwise, you can choose “ON-Demand” if you want to establish TCP connection only when data is required to transmit.

3. **Connection Idle Timeout:** Input the time period of idle timeout. The TCP connection will be terminated if it idles longer than this timeout setting. This option is only available when connection control is set to “ON-Demand”.
4. **Alive Check Timeout:** Input the time period of alive check timeout. The TCP connection will be terminated if it doesn’t receive response of alive-check longer than this timeout setting.
5. **To Host:** Press “Edit” button at right side, and you can enter IP address or FQDN of remote host (TCP server) that you want to communicate.
6. **Remote Port:** Enter the TCP port that remote host (TCP server) is listening.
7. **Definition:** Check this checkbox to enable this rule.

TCP Server Mode

In TCP Server mode, GEM-2M provides a unique IP: Port address on a TCP/IP network. GEM-2M waits passively to be contacted by the host computer, allowing the host computer to establish a connection with and get data from the serial device. This operation mode also supports up to 4 simultaneous connections, so that multiple hosts can collect data from the same serial device -- at the same time.



1. **Operation Mode:** Choose TCP Server.
2. **Listen Port:** Indicate the listening port of TCP connection.

3. **Trust Type:** You can choose “Allow All” to allow all TCP clients to connect, or choose “Specific IP” to limit to certain TCP clients.
4. **Max Connection:** Set the maximum number of concurrent TCP connections. Up to 4 TCP connections can be established at the same time.
5. **Connection Idle Timeout:** Input the time period of idle timeout. The TCP connection will be terminated if it idles longer than this timeout setting.
6. **Alive Check Timeout:** Input the time period of alive check timeout. The TCP connection will be terminated if it doesn’t receive response of alive-check longer than this timeout setting.

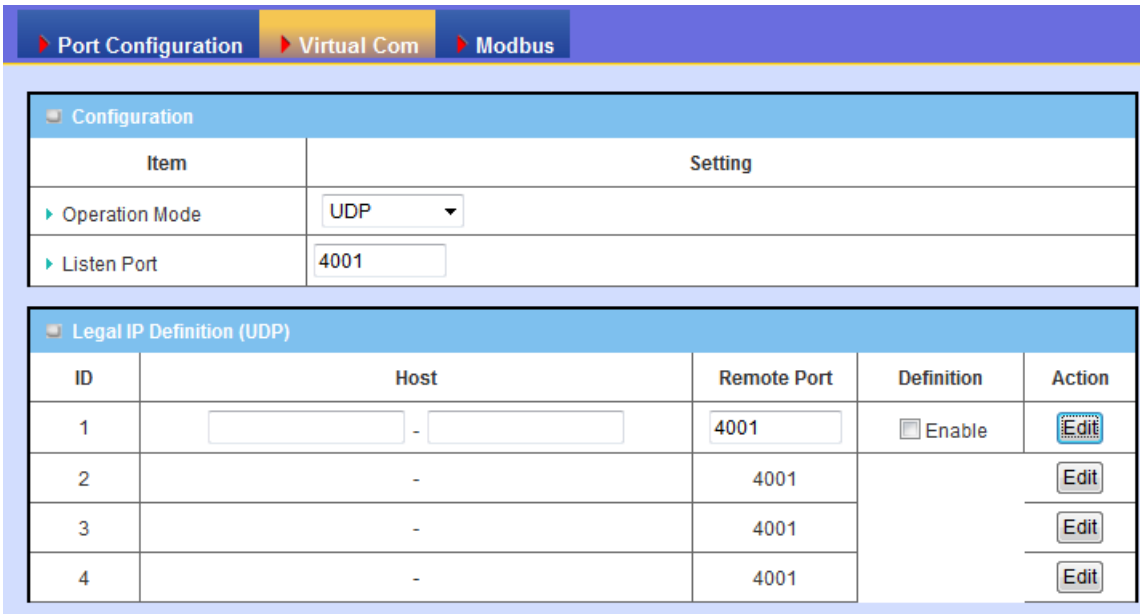
If choosing “Specific IP” in Trust Type, you need to enter the IP address range of allowed TCP clients. Then check the checkbox in “Definition” to enable this rule.

Trusted IP Definition

ID	Host	Definition	Action
1	140.116.82.98 - 140.116.82.100	☑ Enable	Edit
2	-		Edit
3	-		Edit
4	-		Edit

UDP Mode

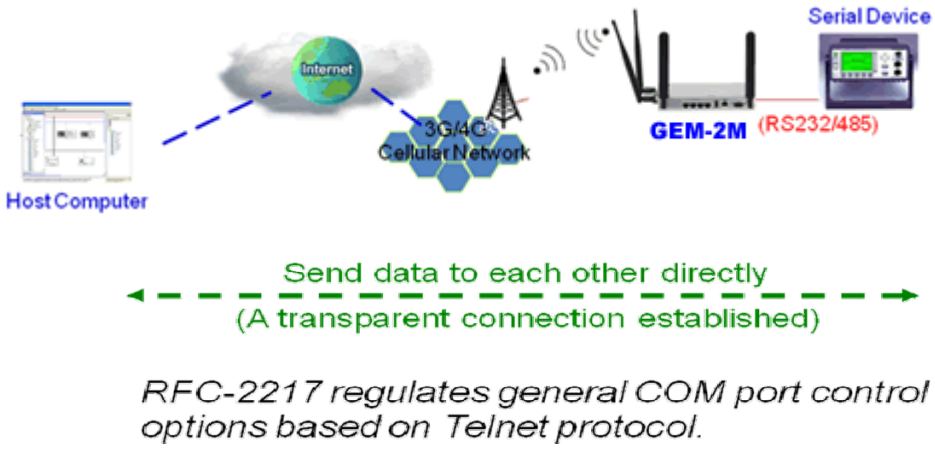
In the UDP mode, you can multicast data from the serial device to multiple host computers, and the serial device can also receive data from multiple host computers, making this mode ideal for message display applications.

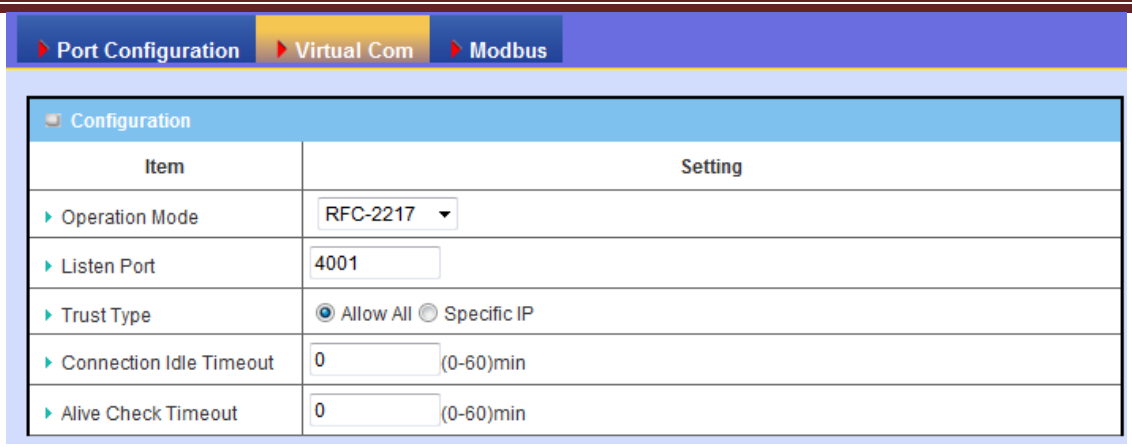


1. **Operation Mode:** Choose UDP.
2. **Listen Port:** Indicate the listening port of UDP connection.
3. **Host:** Press “Edit” button, and enter IP address range of remote UDP hosts.
4. **Remote Port:** Indicate the UDP port of peer UDP hosts.
5. **Definition:** Check this checkbox to enable this rule.

RFC2217 Mode

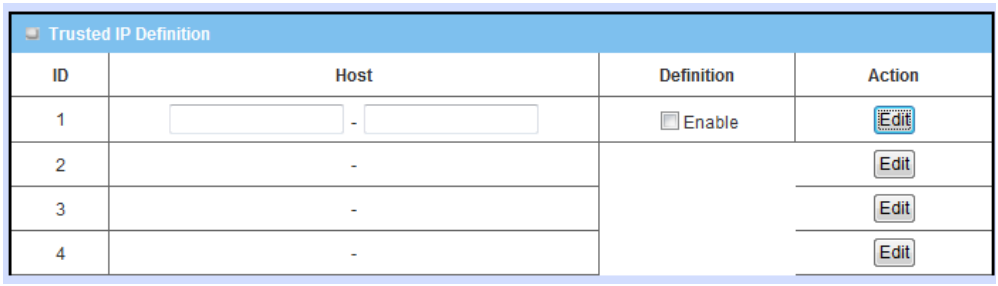
In the RFC2217 mode, it is a standard driver that provides Virtual COM function. RFC2217 defines general COM port control options based on telnet protocol. Any 3rd party driver supporting RFC2217 can be used to implement Virtual COM on the gateway. The driver establishes a transparent connection between host and serial device by mapping the IP: Port of the gateway’s serial port to a local COM port on the host computer.



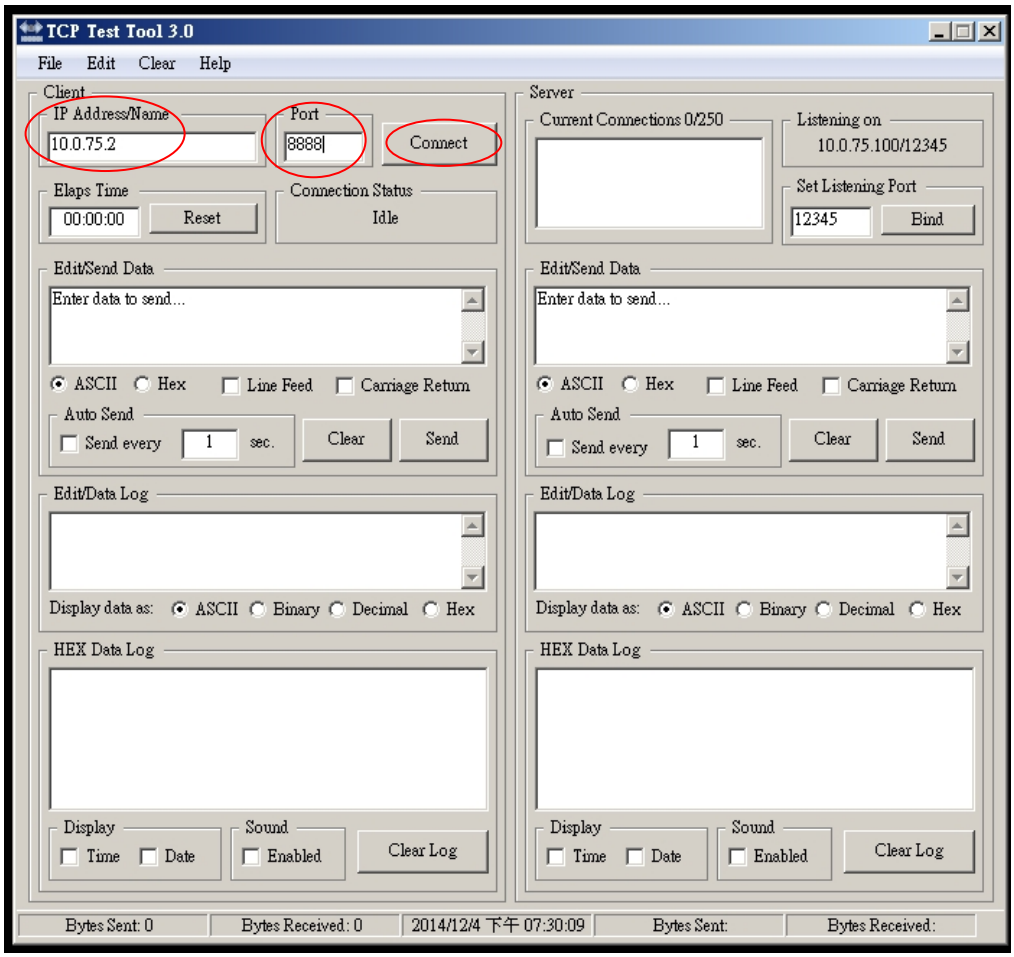


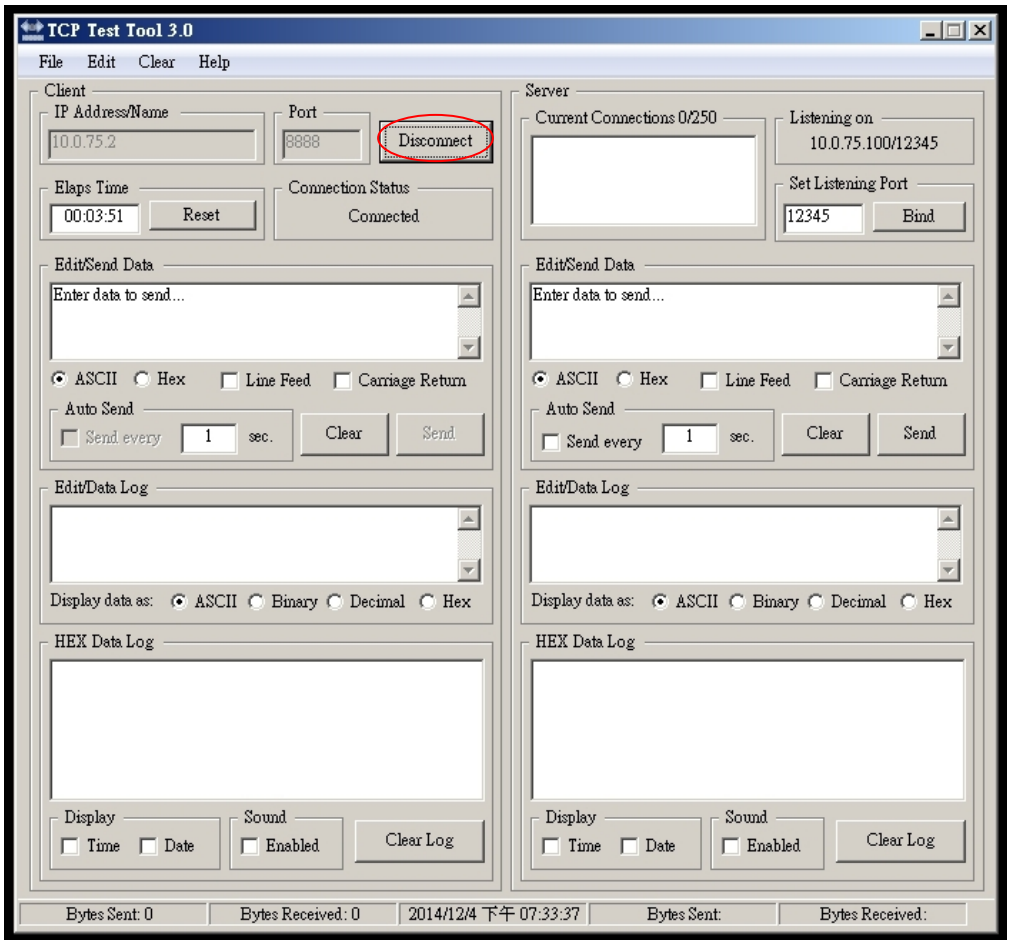
1. **Operation Mode:** Choose RFC-2217.
2. **Listen Port:** Indicate the listening port of RFC-2217 connection.
3. **Trust Type:** You can choose “Allow All” to allow all hosts to connect, or choose “Specific IP” to limit to certain hosts.
4. **Connection Idle Timeout:** Input the time period of idle timeout. The connection will be terminated if it idles longer than this timeout setting.
5. **Alive Check Timeout:** Input the time period of alive check timeout. The connection will be terminated if it doesn’t receive response of alive-check longer than this timeout setting.

If choosing “Specific IP” in Trust Type, you need to enter the IP address range of allowed hosts. Then check the checkbox in “Definition” to enable this rule.



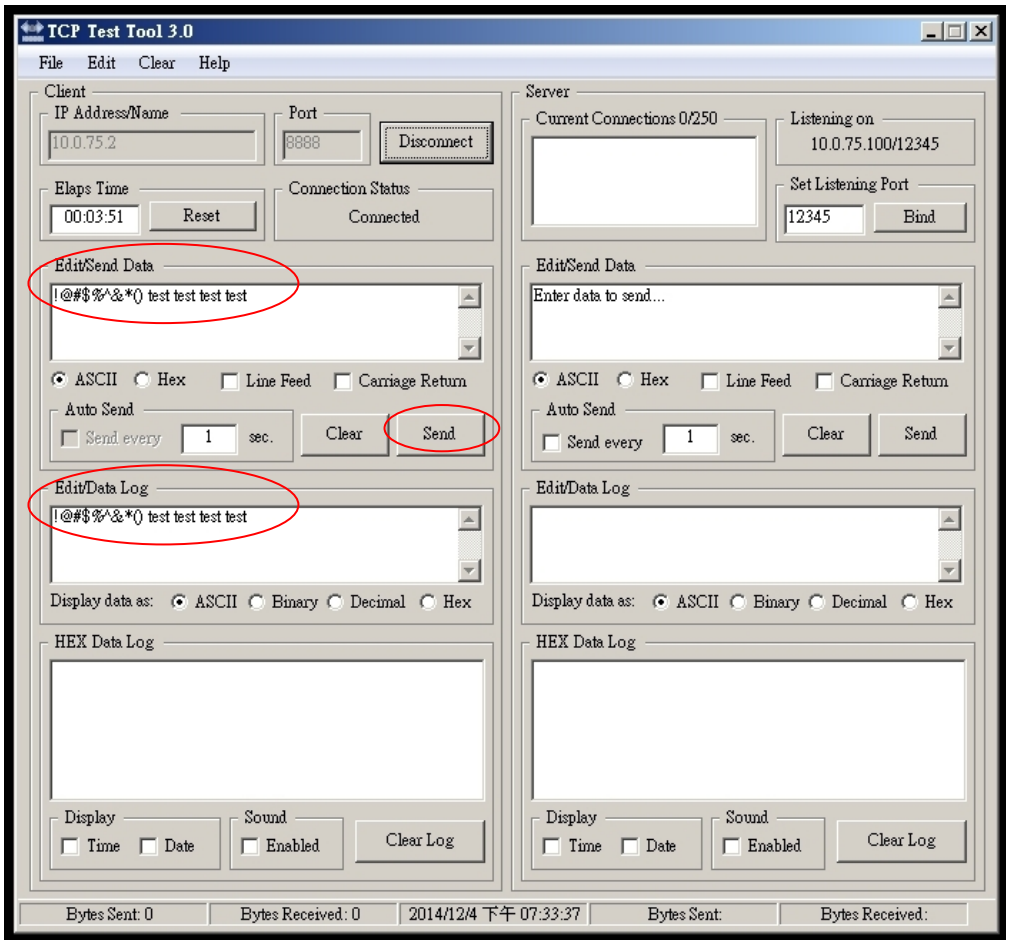
There is another to verify whether the Virtual COM setting is correct or not. You can install the “TPC Test Tool” in another LAN computer.


TCP Test Tool 3.0
File
Edit
Clear
Help
Client
IP Address/Name
10.0.75.2
Port
8888
Connect
Elaps Time
00:00:00
Reset
Connection Status
Idle
Edit/Send Data
Enter data to send...
ASCII
Hex
Line Feed
Carriage Return
Auto Send
Send every
1
sec.
Clear
Send
Edit/Data Log
Display data as:
ASCII
Binary
Decimal
Hex
HEX Data Log
Display
Time
Date
Sound
Enabled
Clear Log
Server
Current Connections 0/250
Listening on
10.0.75.100/12345
Set Listening Port
12345
Bind
Bytes Sent: 0
Bytes Received: 0
2014/12/4 下午 07:30:09
Bytes Sent:
Bytes Received:

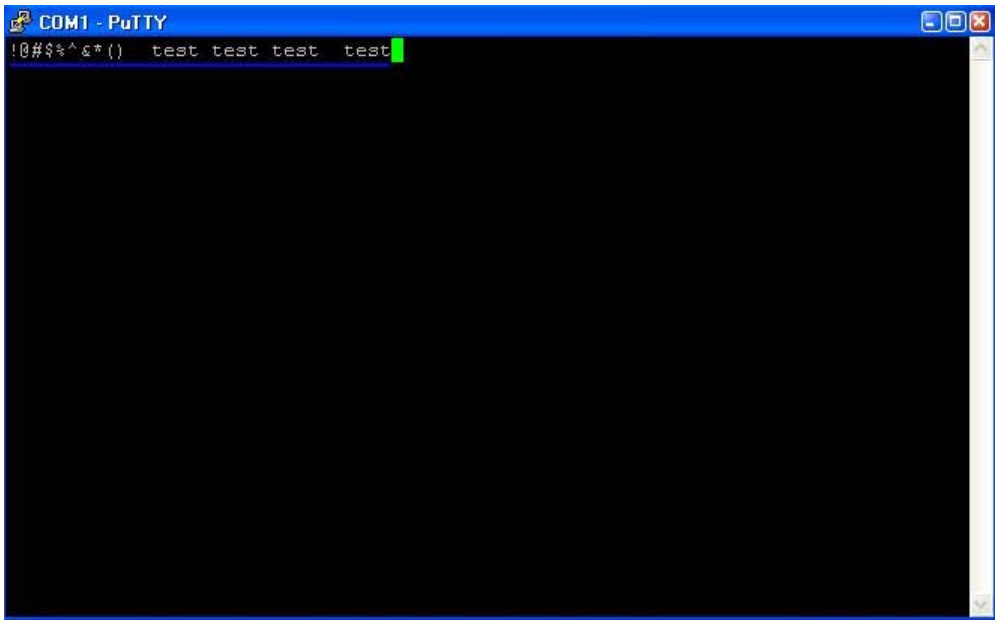


TCP Test Tools can be configured the following steps:

1. IP Address: setting the GEM-2M Gateway address (ex. 192.168.123.254)
2. Port: should be same as the listen port of GEM-2M
3. Click the “Connect” button
4. The Connecting Status should be shown as “Connected”



In the Edit/Send Data, you can try to text some information, and then click the “Send” button.



Then, you can see the same information in the PuTTY.

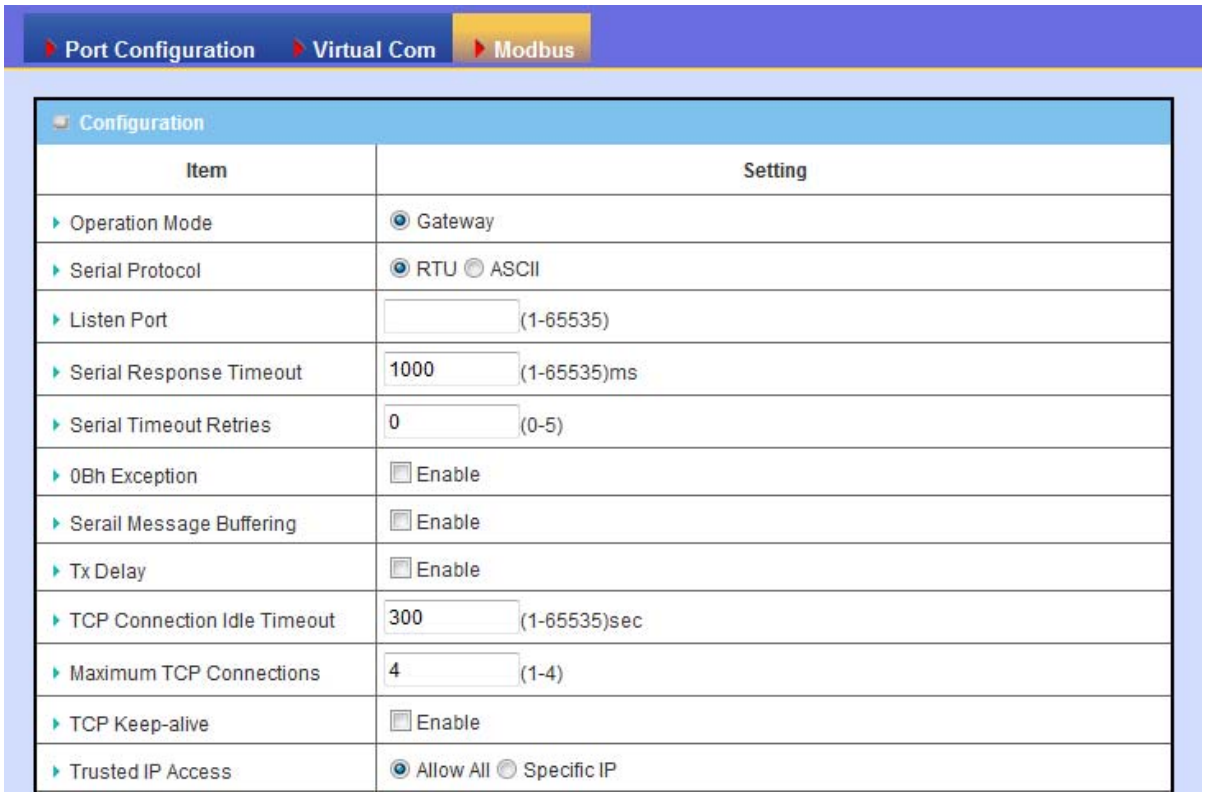
3.2.7.3 Modbus

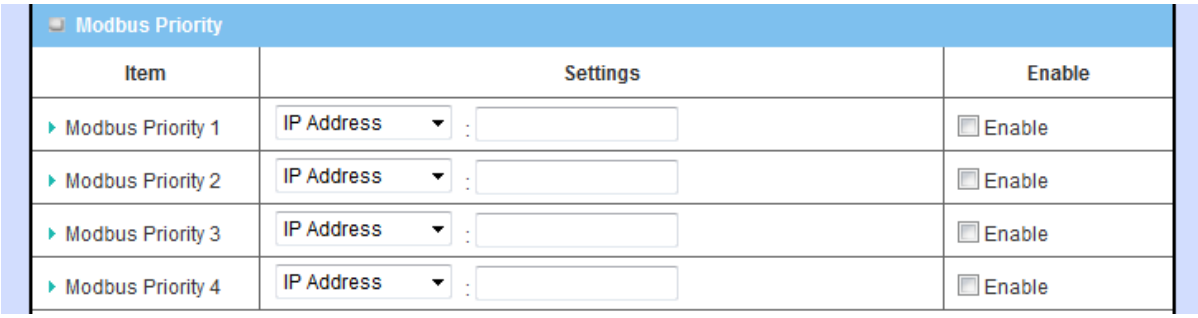
Modbus is one of the most popular automation protocols in the world, supporting traditional RS-232/422/485 devices and recently developed Ethernet devices. Many industrial devices, such as PLCs, DCSs, HMIs, instruments, and meters, use Modbus as the communication standard. It is used to establish master-slave/client-server communication between intelligent devices.

However, the Ethernet-based Modbus protocol is so different from the original serial-based protocols. In order to integrate Modbus networks, the GEM-2M series, including a serial ports that support RS-232 and RS-485 communication interface, can automatically and intelligently translate between Modbus TCP (Ethernet) and Modbus ASCII/RTU (serial) protocols, allowing Ethernet-based PLCs to control instruments over RS-485 without additional programming or effort.

- Integration of Modbus TCP and Modbus RTU/ASCII networks
- Software-selectable RS-232/485 communication.
- High speed serial interface supporting 460.8 Kbps

NOTE: All devices that are connected to a single serial port must use the same protocol (i.e., either Modbus RTU or Modbus ASCII).



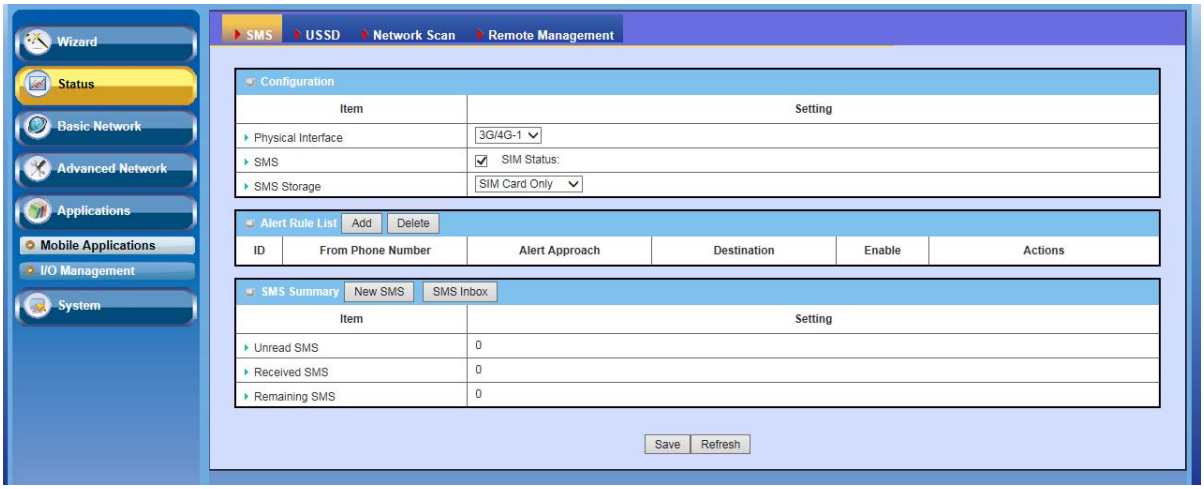


1. **Operation Mode:** the definition of Modbus Gateway is an adapter application enables conversions between Serial and Network Modbus protocols.
2. **Serial Protocol:** defines the Modbus protocol used on the serial communication.
3. **Listen Port:** defines the TCP or UDP port that Masters can make connections to.
4. **Serial Response Timeout:** if the serial side does not response within the specific time, data would be dropped and not transmitted over TCP even if the gateway receives it later (if the response is not received, the gateway can generate and return the Master exception)
5. **Serial Timeout Retries:** If "0" is set, the gateway would not store TCP packets in the buffer. If the number is greater than "0", the gateway would store the TCP packets in the buffer and retries the specified time when the Modbus device on the serial side does not response.
6. **0Bh Exception:** Modbus protocol defines that the 0Bh is “an error code which means error message of the interconnected gateway, or no response of the access device”. When the Modbus slave device does not respond before the timeout has been reached or has a bad response (check sum does not match), the 0Bh exception code is transmitted to the master that initiated the Modbus message.
7. **Serial Message Buffering:** if this option is selected, the gateway will buffer TCP up to 32 requests. If this option is unselected, the gateway will respond with a 06h if it has a message out on the port with no response yet.
8. **Tx Delay:** this is the minimum amount of time after receiving a response before the next message can be sent out.
9. **TCP Connection Idle Timeout:** idle timeout in seconds for the Modbus /TCP connection. If the gateway doesn't receive any Modbus /TCP query within the specific time, the connection will be closed.
10. **Maximum TCP Connection:** maximum of four simultaneous Modbus /TCP connections is allowed
11. **TCP Keep-alive:** enable the connection testing enabled for TCP network communication
12. **Trusted IP Access:** defines the IP that is allowed to connect to the gateway
13. **Modbus Priority:** defines the priorities from specific IP, or Modbus ID or

Function Code can be proceeding in high priority..

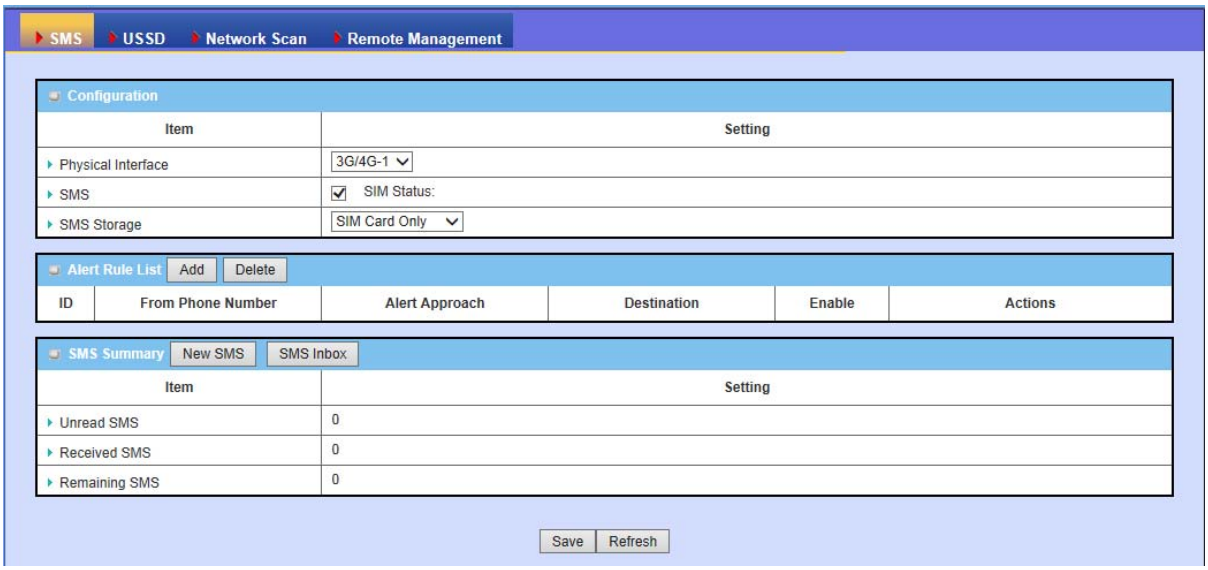
3.3 Applications

In this section you can finish the Mobile Application settings. This device is equipped with a 3G/4G module as WAN interface, and it also provide the SMS, USSD, Network Scan and SMS-based Remote Management. Besides, there is one “I/O Management” function to define the mapping between events and handlers.



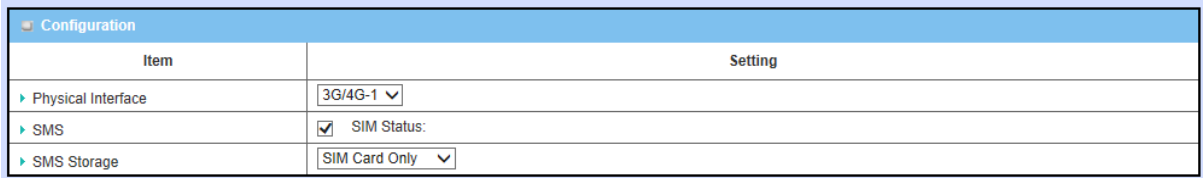
3.3.1 Mobile Applications

3.3.1.1 SMS



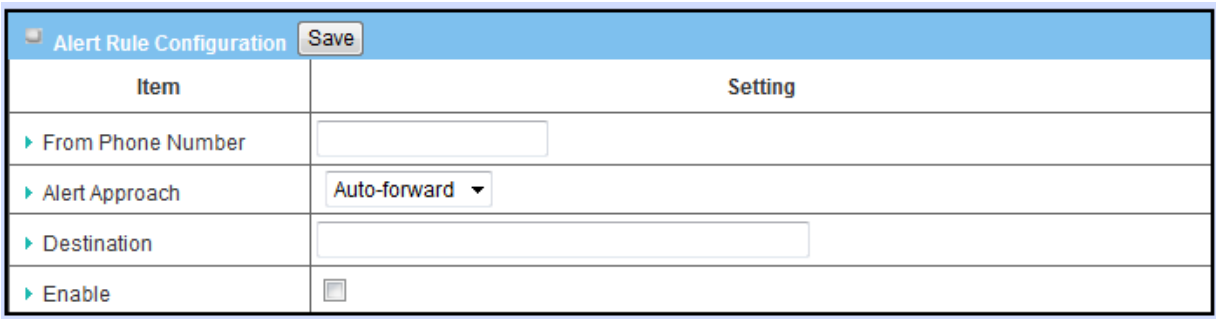
You can compose new SMS message and check received SMS message on this

gateway.



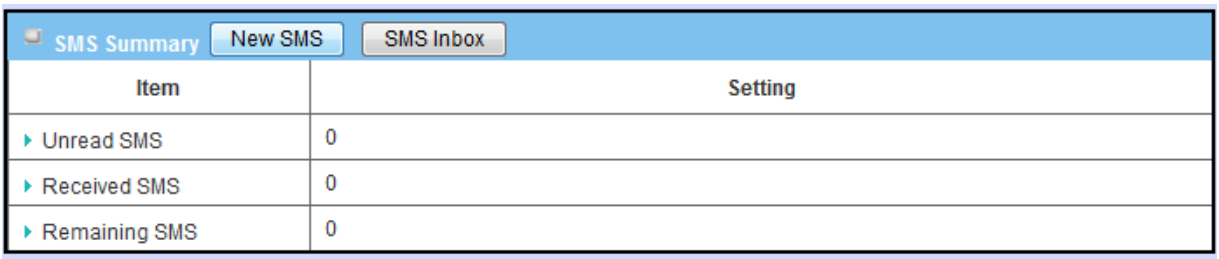
1. **Physical Interface:** Indicate which 3G/LTE modem is used for SMS feature.
2. **SMS:** Indicate which SIM card is used for SMS feature.
3. **SMS Storage:** Select storage for SMS message. This gateway only supports “SIM Card Only” for SMS storage.

This gateway can forward received SMS message automatically. Press “Add” to add new rule.



1. **From Phone Number:** Indicate phone number of sender.
2. **Alert Approach:** Decide the way to forward message. You can forward this message to another phone number, or to a mail address, or to a syslog server.
3. **Destination:** Please enter the phone number of receiver if you choose “Auto-forward”. Or enter a mail address if choosing “By Email”. Or enter the IP address of syslog server if choosing “By Syslog”.
4. **Enable:** Enable this rule.

SMS Summary

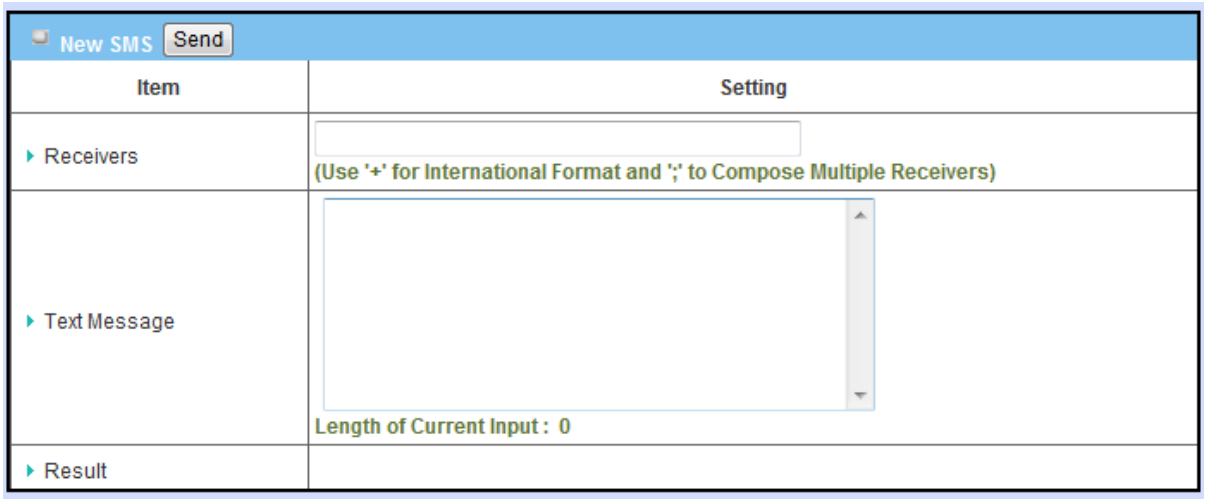


1. **Unread SMS:** Indicate number of unread SMS message.

2. **Received SMS:** Indicate number of total received SMS message.
3. **Remaining SMS:** Indicate number of new message can be received because of SMS storage limit.

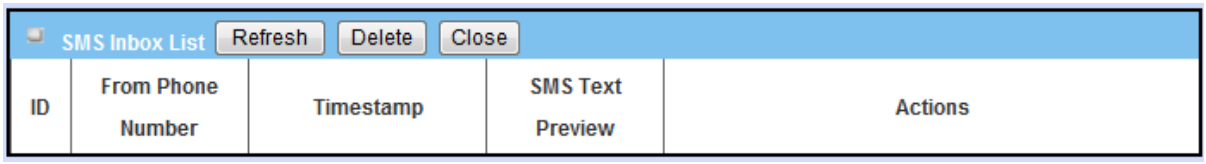
Create New SMS Message

You can create a new SMS message on this page. After finishing the content of message, and filling with phone number of receiver(s), you can press the “Send” button to send this message out. You can see “Send OK” if the new message has been sent successfully.



Read New SMS Message

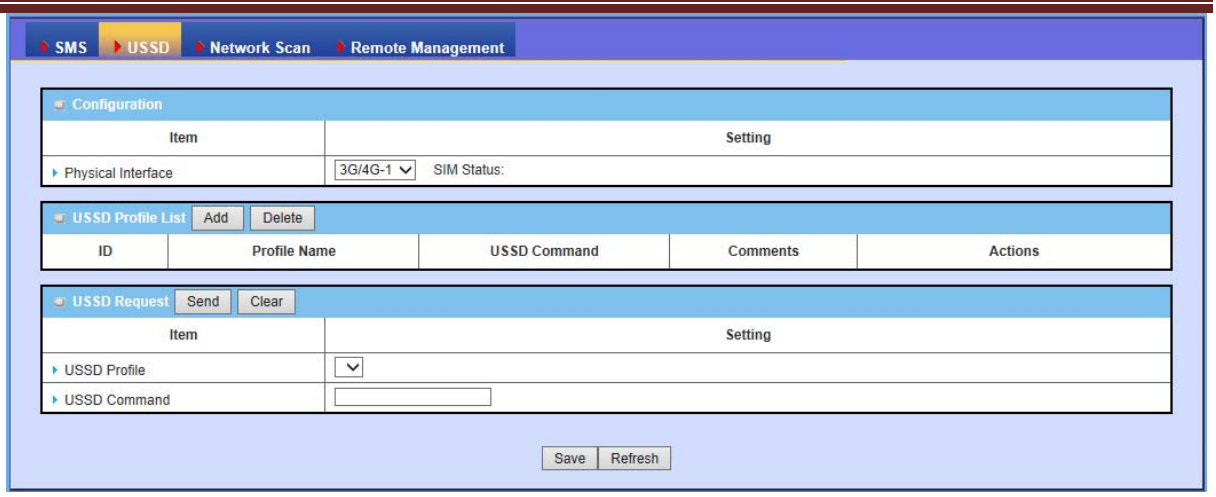
You can read, delete, reply, and forward messages in this inbox section.



1. **Refresh:** You can press “Refresh” button to renew SMS lists.
2. **Delete, Reply, Forward Messages:** After reading message, you can check the checkbox on the right of each message to delete, reply, or forward this message.

3.3.1.2 USSD

Unstructured Supplementary Service Data (USSD) is a protocol used by GSM cellular telephones to communicate with the service provider's computers. USSD can be used for prepaid callback service, mobile-money services, location-based content services, and as part of configuring the phone on the network.



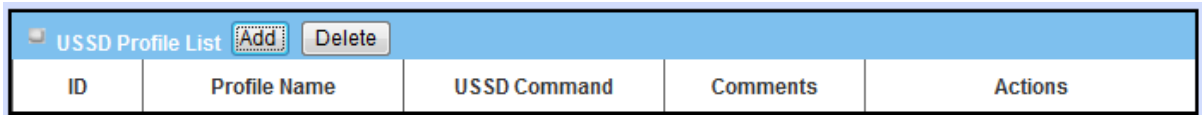
USSD Configuration

You can compose a USSD message, and sends it to the service provider, where it is received by a computer dedicated to USSD. The answer from this computer is sent back to this device, but it is usually with a very basic presentation.

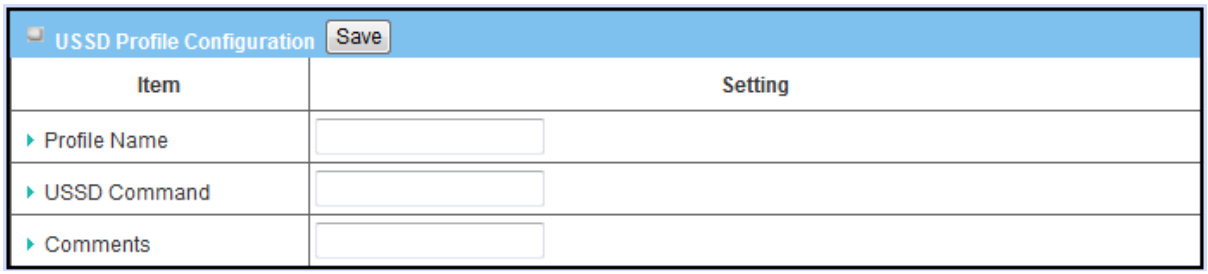
1. **Physical Interface:** Indicate which 3G/LTE modem is used for USSD feature. And SIM Status indicates which SIM card is used for USSD feature.

USSD Profile List

You can edit USSD profile for some common used command. Press “Add” button to add new profile. And select some existed profiles to delete by clicking on “Delete” button.

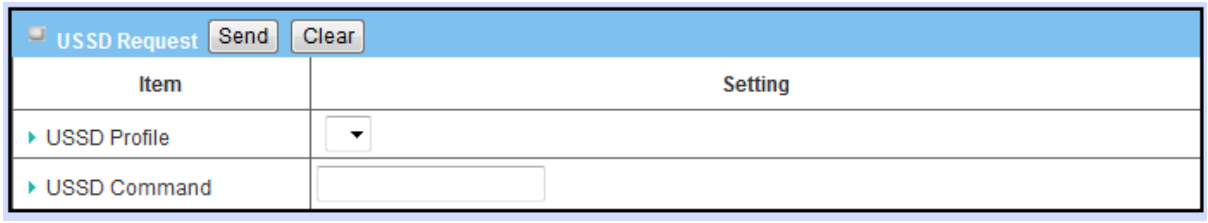


USSD Profile Configuration



1. **Profile Name:** Indicate name of this profile.
2. **USSD Command:** Type USSD command of this profile.
3. **Comments:** Add comments for this profile.

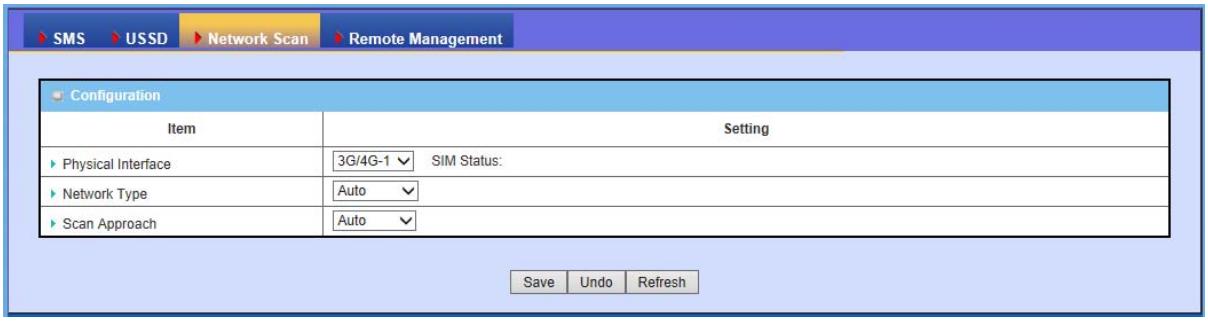
Send USSD Command



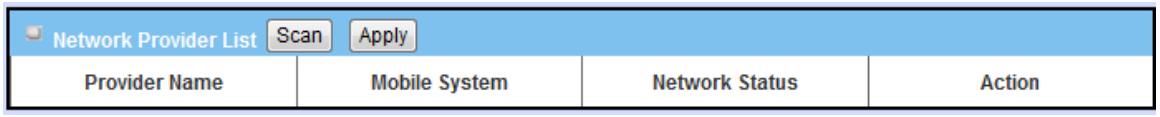
You can select USSD command from existed profile or type command manually. Then press “Send” button to send out USSD command.

3.3.1.3 Network Scan

This part is for 3G/LTE cellular network scan. Usually, this part would be done automatically. Manual scan is used for problem diagnosis.



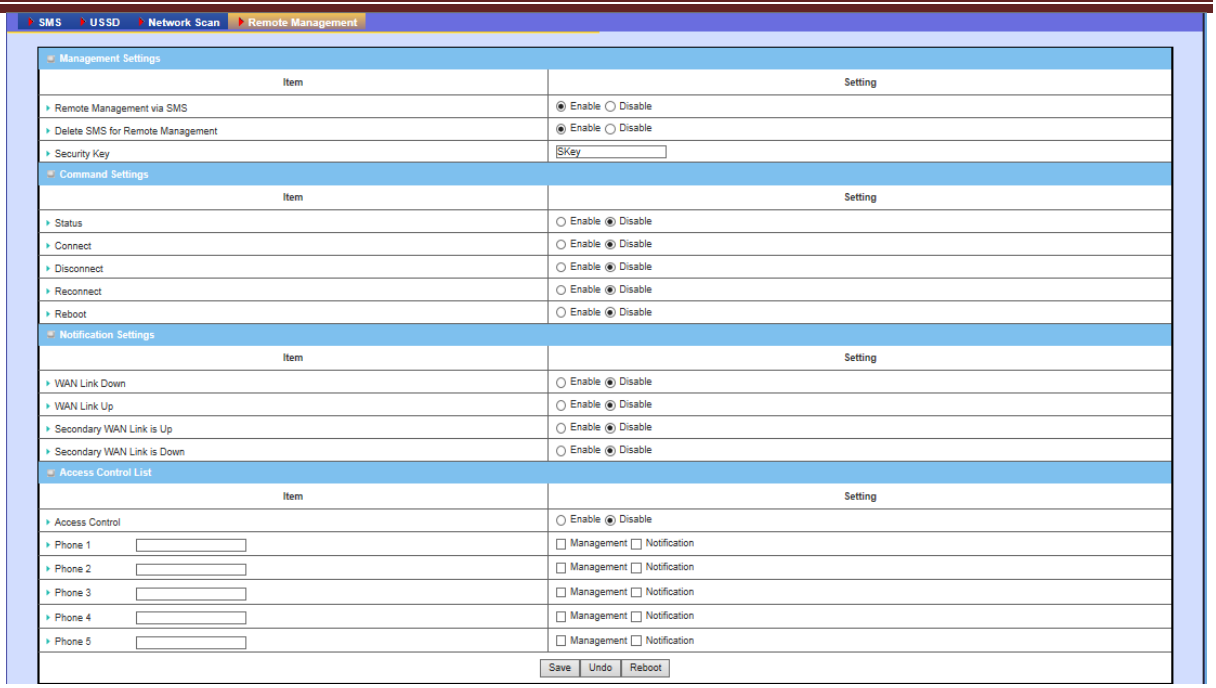
1. **Physical Interface:** Indicate which 3G/LTE modem is used for network scan. And SIM Status indicates which SIM card is used to Network Scan.
2. **Network Type:** Set network type of network scan. You can choose “2G Only”, “3G Only”, “LTE Only”, or “Auto”.
3. **Scan Approach:** You can choose “Auto” or “Manually”. If you choose “Manually”, press “Scan” button to scan cellular network nearby in your environment and select one network provider to apply by clicking on the “Apply” button.



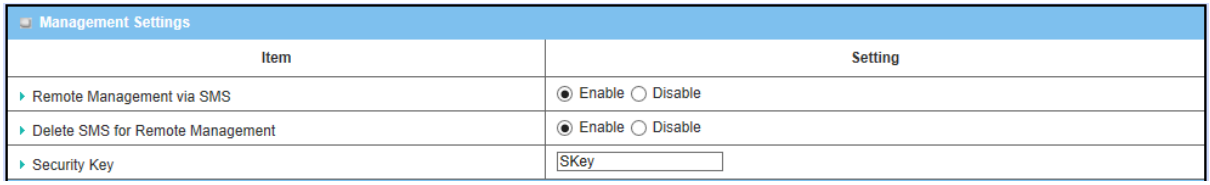
Note. Incorrect setting here may cause 3G/LTE connection problems.

3.3.1.4 Remote Management

This part is for remote management functions that are done by text SMS (Short Message Service). Users can send certain SMS to this gateway to activate some actions, such as connect/disconnect/reconnect WAN connection or reboot the system. Besides, gateway can also send SMS to users to alert some events automatically.



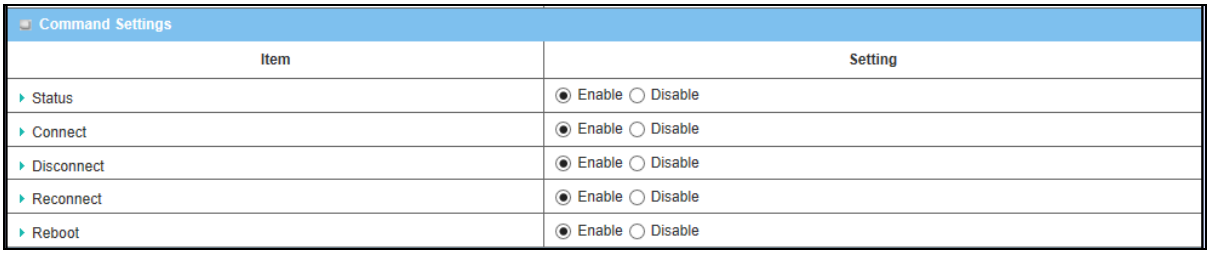
Management Settings



1. **Remote Management via SMS:** Check this to enable this function.
2. **Delete SMS for Remote Management:** This device will delete received SMS message that is for remote management purpose if enabling this option. This option can prevent storage space of SIM card from being occupied continuously. If SIM storage is full, this gateway can't receive any new SMS.
3. **Security Key:** This security key will be used for authentication when this gateway receives SMS command. Users need to type this key first and then followed by a command. There should be a "blank" between key and command (e.g. 1234 reboot). If this field is empty, users just need to type command without adding any key information.

Note. If security key is empty, access control needs to be activated. The security key can be empty if access control is activated.

Command Settings



1. **Status:** Enable it, and you can send command "status" to query WAN connection

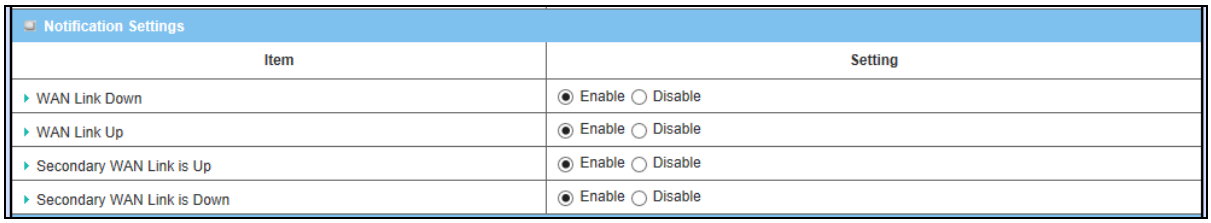
status. For 3G/LTE WAN, router will send back WAN IP address, network name, network type, and connection time via SMS. For Ethernet WAN, router will send back WAN IP address and connection time via SMS. The content would be similar to following format:

WAN IP: [xxx.xx.xxx.xx]
Network: [carrier name] (for wireless WAN only)
Type: [GPRS, WCDMA, HSPA, HSPA+, LTE] (for wireless WAN only)
Conn. Time: [connection time]

2. **Connect**: Enable it, and you can send command "**connect**" to start WAN connection.
3. **Disconnect**: Enable it, and you can send command "**disconnect**" to disconnect WAN connection.
4. **Note**. If this gateway receives "disconnect" command from SMS, it won't try to connect again no matter WAN connection mode is set to auto-reconnect.
5. **Reconnect**: Enable it, and you can send command "**reconnect**" to disconnect WAN connection, and start WAN connection again immediately.
6. **Reboot**: Enable it, and you can send command "**reboot**" to restart router.

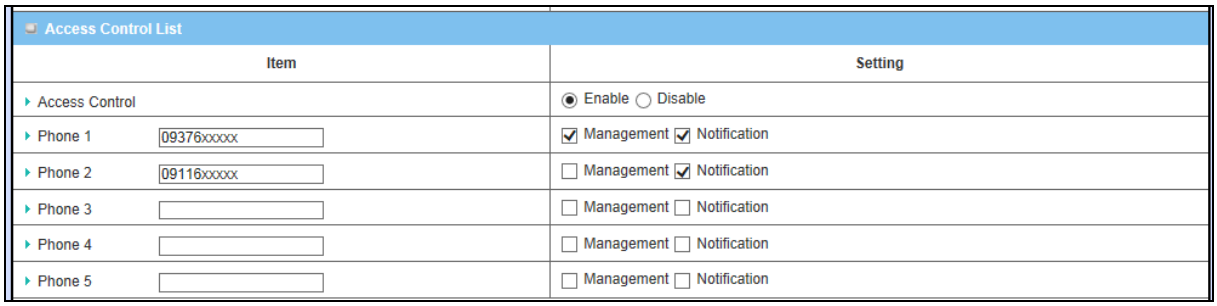
All management commands are not case sensitive

Notification Settings



1. **WAN Link Down**: Enable it, and this gateway will send a message to users if primary WAN connection is dropped.
2. **WAN Link Up**: Enable it, and this gateway will send a message to users if WAN connection is established. This message will also include WAN IP address.
3. **Secondary WAN is Up**: Enable it, and this gateway will send a message to users if secondary WAN is connected. This message will also include WAN IP address.
4. **Secondary WAN is Down**: Enable it, and this gateway will send a message to users if secondary WAN is disconnected.

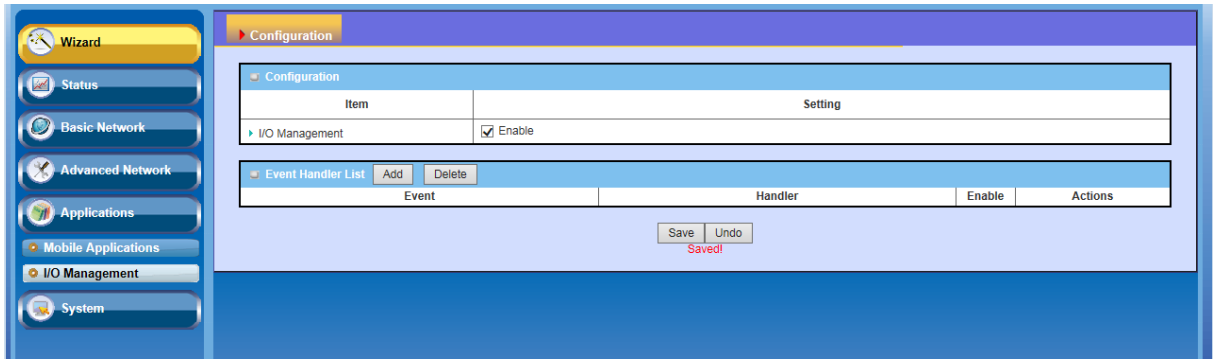
Access Control List



1. **Access Control**: Users can decide which phone number can send commands to this gateway or receive notifications when enable this option.
2. **Phone 1~5**: For security concern, this gateway won't deal with the command if that phone number is not in the list even the security key is correct. The phone number must be with the international prefix (i.e. +886939123456). You can also assign specific phone number can send command and/or also can receive notifications.

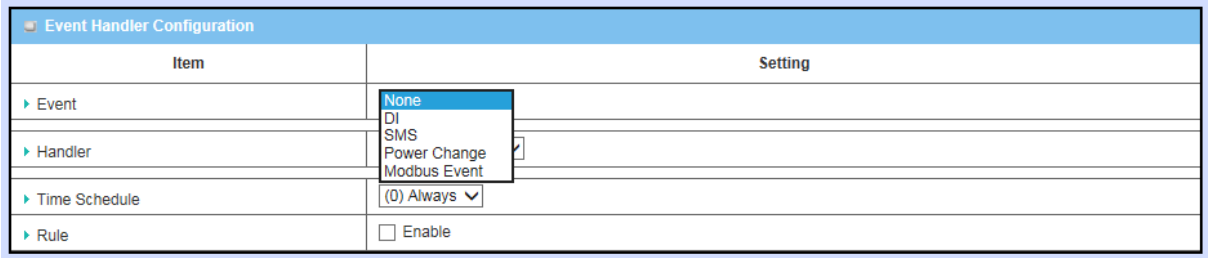
3.3.2 IO Management

This IO management is to help user to define DIDO events / handlers behavior. Once you enable the IO management, you can add some Event / Handler pairs to follow your requirements.

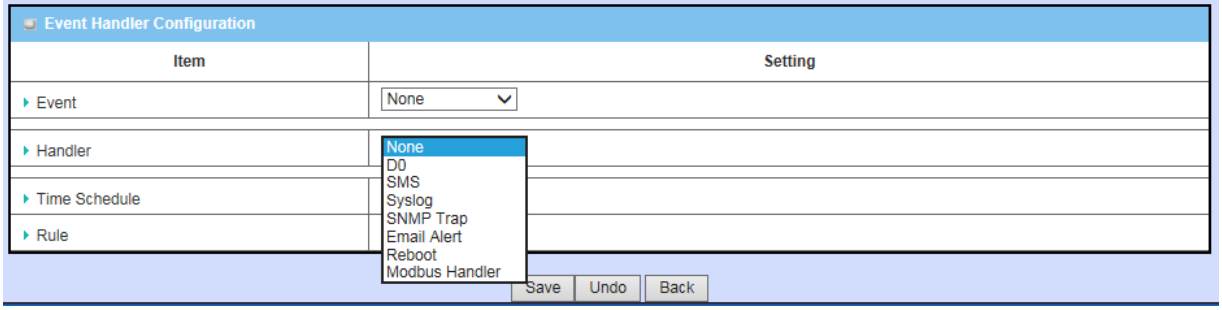


3.3.2.1 Configuration

To press 'Add' button, you can enter the following page, and define your event as DI / SMS / Power Change / Modbus Event. Some event categories depend on product models.

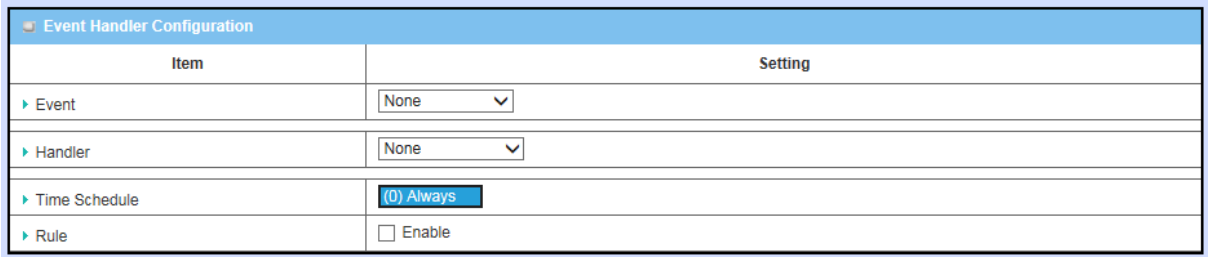


Then, you can define the handler behavior for None / DO / SMS / Syslog / SNMP Trap / Email Alert / Reboot / Modbus Handler. Some handler categories depend on product models.



As for the Time schedule, it is to allow Event/ Handler to active by the Time Schedule Rule. The feature depends on product models.

To activate the Event / Handler pair to work by checking the "Enable" box.



3.4 System

In the System section you can check system related information and execute some system operations, define some time schedule rules, make object grouping, define external server objects and configure the operation parameters on Web UI surfing.

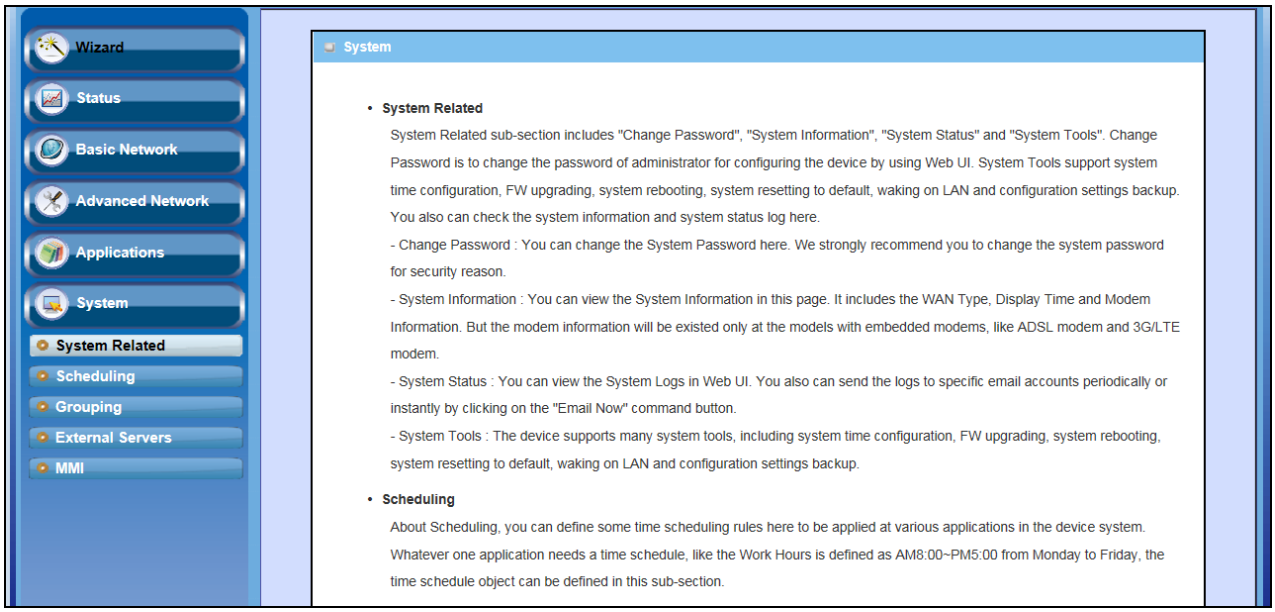
About system related, you can see system related information and system logs, use system tools for system update and do some network tests.

About Scheduling, you can define some time scheduling rules here to be applied at various applications in the device system. Whatever one application needs a time schedule, like the "Work Hours" is defined as AM8:00~PM5:00 from Monday to Friday, the

time schedule object can be defined in the **[System]-[Scheduling]** section.

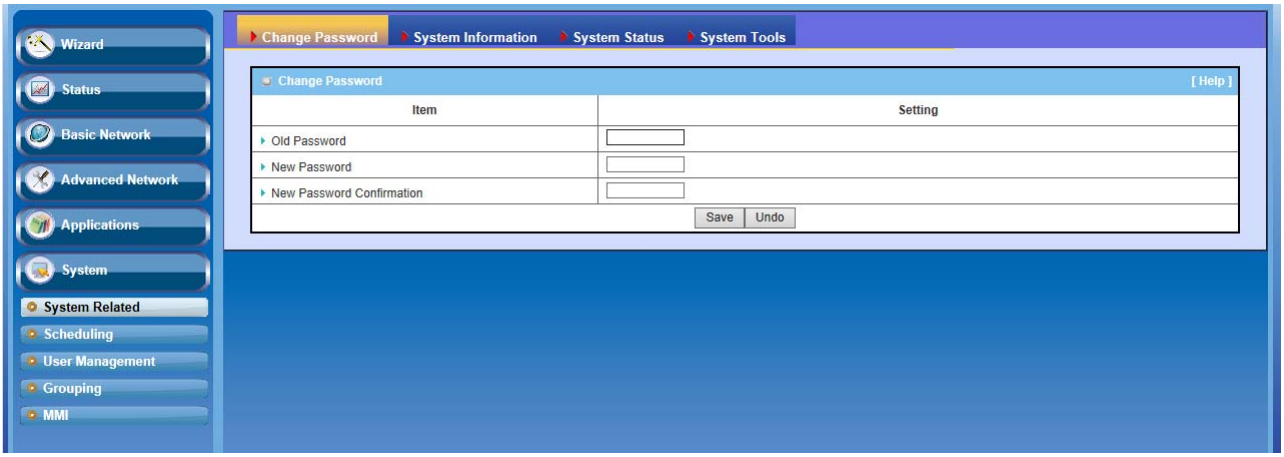
About External Servers, you can define some external server objects here to be applied at various applications in the device system. Whatever one application needs an external server, like a RADIUS server, the external server object can be defined in the **[System]-[External Servers]** section. These server objects include Email Server objects, Syslog Server objects, RADIUS Server objects, Active Directory Server objects, LDAP Server objects and UAM Server objects.

About MMI (Man-Machine Interface), it means the Web-based GUI. User can set the administrator timeout of Web UI surfing during configuring the device by the administrator.


Wizard
Status
Basic Network
Advanced Network
Applications
System
System Related
Scheduling
Grouping
External Servers
MMI
System
System Related
System Related sub-section includes "Change Password", "System Information", "System Status" and "System Tools". Change Password is to change the password of administrator for configuring the device by using Web UI. System Tools support system time configuration, FW upgrading, system rebooting, system resetting to default, waking on LAN and configuration settings backup. You also can check the system information and system status log here.
- Change Password : You can change the System Password here. We strongly recommend you to change the system password for security reason.
- System Information : You can view the System Information in this page. It includes the WAN Type, Display Time and Modem Information. But the modem information will be existed only at the models with embedded modems, like ADSL modem and 3G/LTE modem.
- System Status : You can view the System Logs in Web UI. You also can send the logs to specific email accounts periodically or instantly by clicking on the "Email Now" command button.
- System Tools : The device supports many system tools, including system time configuration, FW upgrading, system rebooting, system resetting to default, waking on LAN and configuration settings backup.
Scheduling
About Scheduling, you can define some time scheduling rules here to be applied at various applications in the device system. Whatever one application needs a time schedule, like the Work Hours is defined as AM8:00~PM5:00 from Monday to Friday, the time schedule object can be defined in this sub-section.

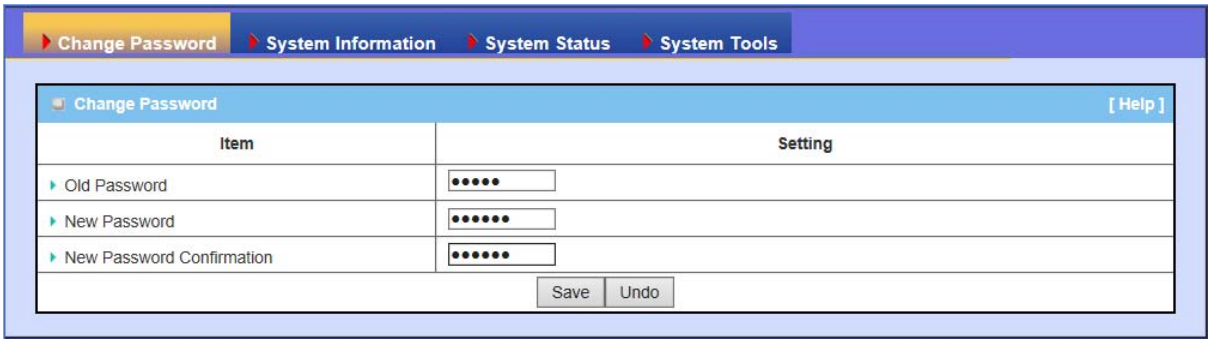
3.4.1 System Related

System Related section includes “Change Password”, “System Information”, “System Status” and “System Tools”. Change Password is to change the password of administrator for configuring the device by using Web UI. System Tools support system time configuration, FW upgrading, system rebooting, system resetting to default, waking on LAN and configuration settings backup. You also can check the system information and system status log here.



3.4.1.1 Change Password

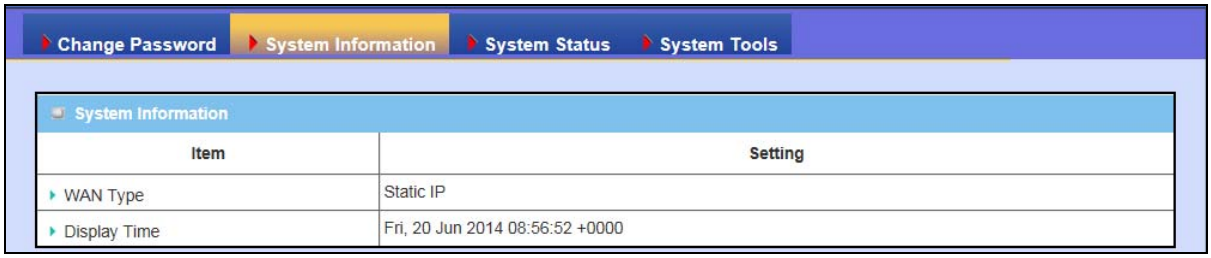
You can change the System Password here. We strongly recommend you to change the system password for security reason. Click on “Save” to store your settings or click “Undo” to give up the changes.



1. **Old Password:** Input the old password of administrator.
2. **New Password:** Input the new password of administrator for future logging in. Certainly, once the password is changed successfully, system will ask you login again with new password.
3. **New Password Confirmation:** Re-type new password again here. It must be the same as the one in “New Password”; otherwise, an error message will be shown out.

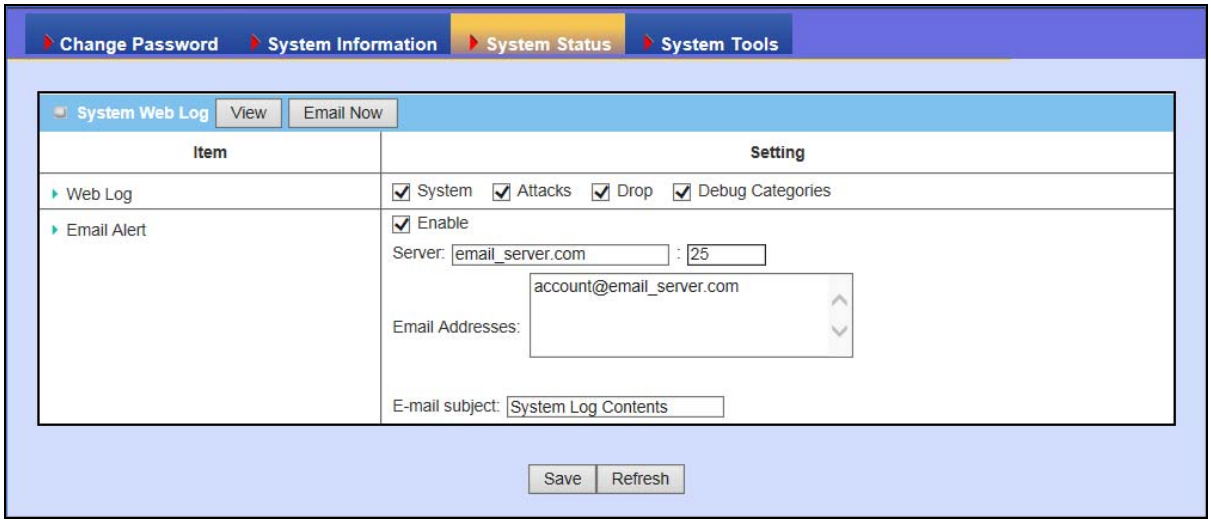
3.4.1.2 System Information

You can view the System Information in this page. It includes the WAN Type, Display Time and Modem Information. But the modem information will be existed only at the models with embedded modems, like ADSL modem and 3G/LTE modem.



3.4.1.3 System Status

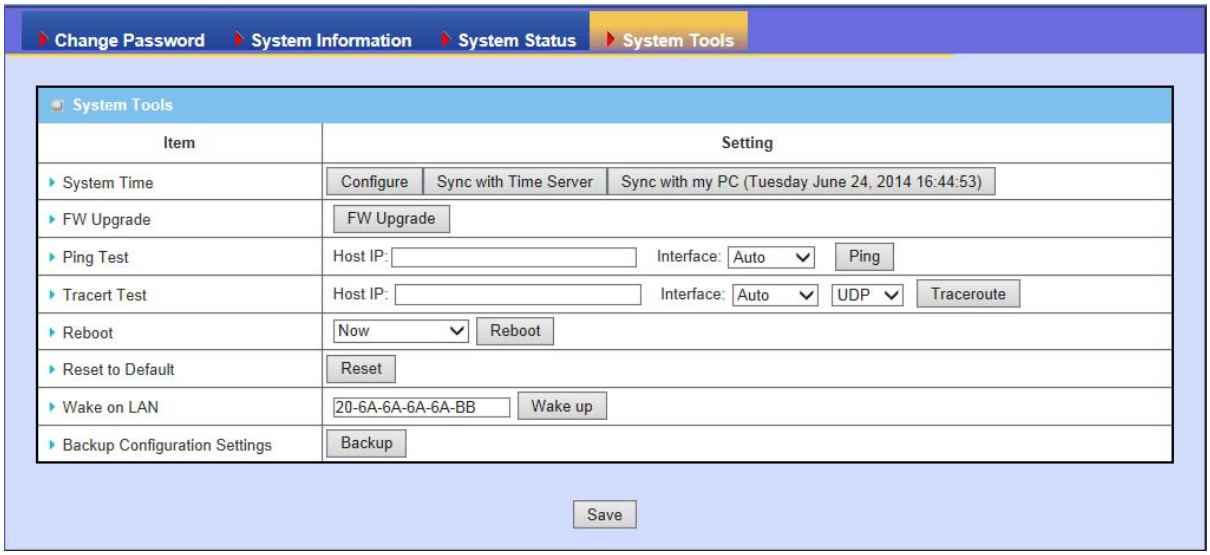
You can view the System Logs in Web UI. You also can send the logs to specific email accounts periodically or instantly by clicking on the “Email Now” command button.



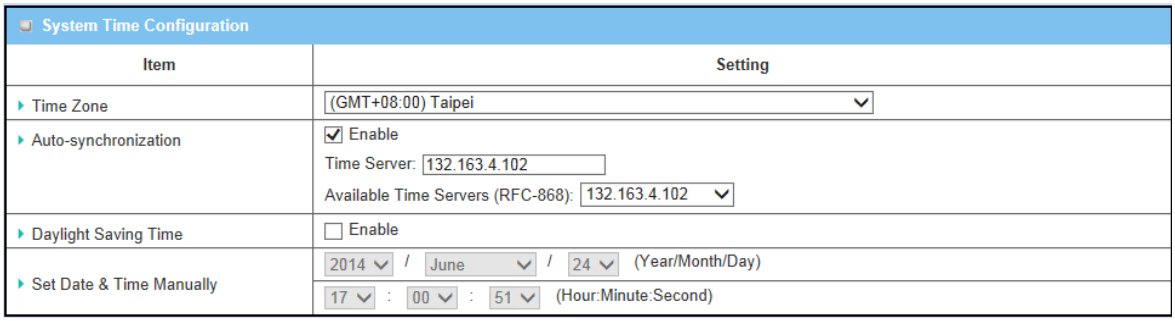
1. **Web Log**: You can select the log types to be collected in the web log area. There are “System”, “Attacks”, “Drop”, and “Debug” types of system logs for you to select.
2. **View**: You can browse, refresh, download, and clear the log messages after clicking on the “View” command button.
3. **Email Alert**: This device can also export system logs via sending emails to specific recipients. The items you have to setup include:
   * **Enable**: Check it if you want to enable Email alert (send system logs via email).
   * **Server: Port**: Input the SMTP server IP and port, which are connected with ':'. If you do not specify port number, the default value is 25.
   * **E-mail Addresses:** The recipients are the ones who will receive these logs. You can assign more than 1 recipient by using ';' or ',' to separate these email addresses.
   * **E-mail Subject**: The subject of email alert is optional.
4. **Email Now:** A command button to let you email out current web logs right now instead of the email alert period.

3.4.1.4 System Tools

The device supports many system tools, including system time configuration, FW upgrading, system rebooting, system resetting to default, waking on LAN and configuration settings backup.



1. **System Time**: There are three approaches to setup the system time. Before the process, some basic information must be filled by clicking on the "Configure" command button. Basic information includes following items:

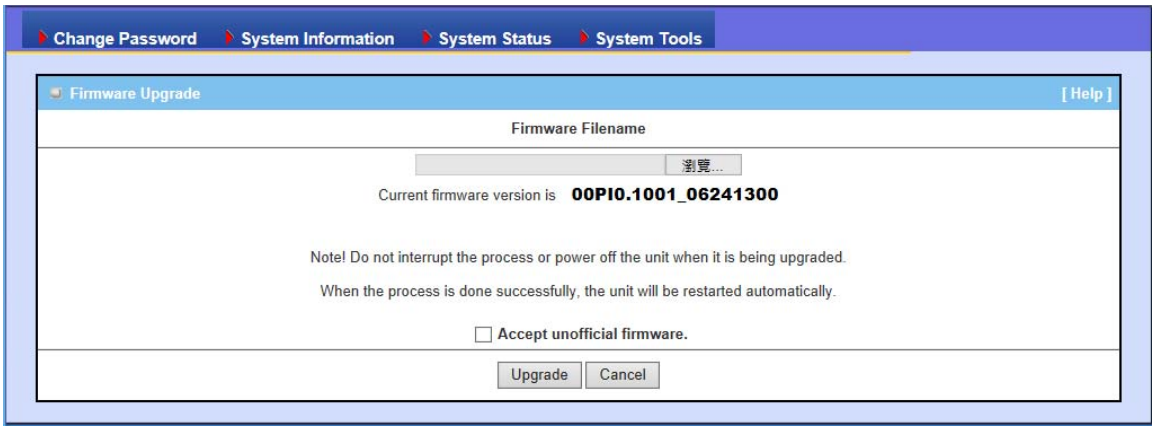


   a. **Time Zone**: Select a time zone where this device locates.
   b. **Auto-Synchronization**: Check the "Enable" checkbox to enable this function. Besides, you can select a NTP time server to consult UTC time from the available list and by default, it is 132.163.4.102.
   c. **Daylight Saving Time:** Check the "Enable" checkbox to enable this function.
   d. **Set Date & Time Manually:** Set the date and time for system by manual. But Auto-Synchronization must be unchecked beforehand to do it.

   Above is the first way to setup system date and time. That is, it is the manual way. The second way is "Sync with Timer Server". Based on your selection of time server in basic information configuration, system will communicate with time server by NTP Protocol to get system date and time after you click on the button.

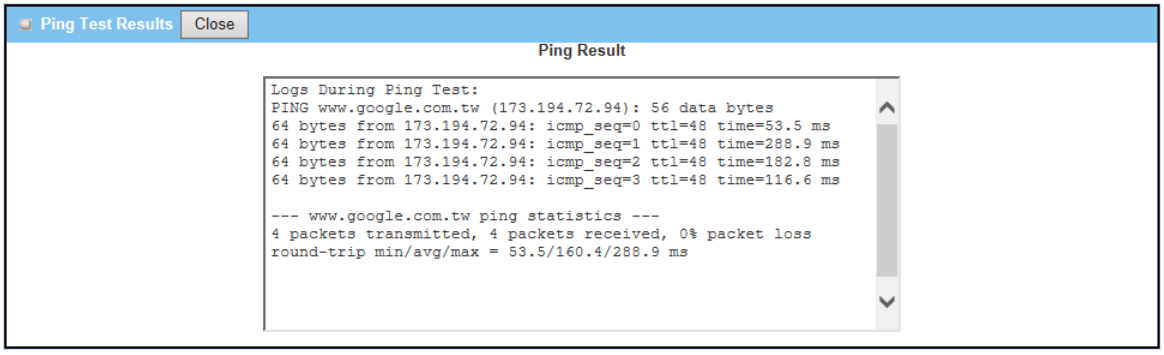
The last way is “Sync with my PC”. Click on the button to let system synchronizes its date and time to the ones of the configuration PC.

2. **FW Upgrade:** If new firmware is available, you can upgrade router firmware through the WEB GUI here. After clicking on the “FW Upgrade” command button, you need to specify the file name of new firmware by using “Browse” button, and then click “Upgrade” button to start the FW upgrading process on this device. If you want to upgrade a firmware which is from GPL policy, please check “Accept unofficial firmware”.



NOTE. PLEASE DO NOT TURN THE DEVICE OFF WHEN UPGRADE IS PROCEEDING.

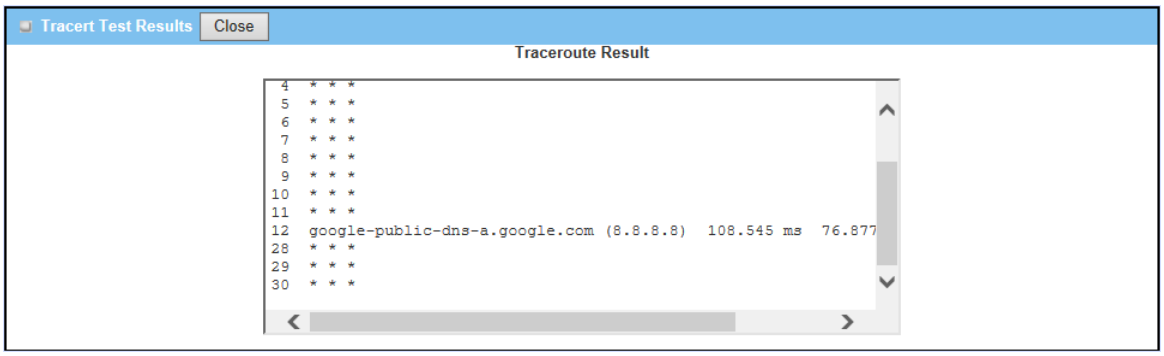
3. **Ping Test**: This allows you to specify an IP / FQDN and the test interface, so system will try to ping the specified device to test whether it is alive after clicking on the “Ping” button. A test result window will appear beneath it. There is a “Close” command button there can let the test result windows disappear.


Ping Test Results
Close
Ping Result
Logs During Ping Test:
PING www.google.com.tw (173.194.72.94): 56 data bytes
64 bytes from 173.194.72.94: icmp_seq=0 ttl=48 time=53.5 ms
64 bytes from 173.194.72.94: icmp_seq=1 ttl=48 time=288.9 ms
64 bytes from 173.194.72.94: icmp_seq=2 ttl=48 time=182.8 ms
64 bytes from 173.194.72.94: icmp_seq=3 ttl=48 time=116.6 ms
--- www.google.com.tw ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 53.5/160.4/288.9 ms

4. **Tracert Test**:

Trace route command is a network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an IP network. Trace route proceeds unless all (three) sent packets are lost more than twice, then the connection is lost and the route cannot be evaluated. Ping, on the other hand, only computes the final round-trip times from the destination point. First, you need to specify an IP / FQDN, the test interface and used protocol number. Used protocol number is either “UDP” or “ICMP”, and by default, it is “UDP”. Then,

system will try to trace the specified device to test whether it is alive after clicking on the “Traceroute” button. A test result window will appear beneath it. There is a “Close” command button there can let the test result windows disappear.

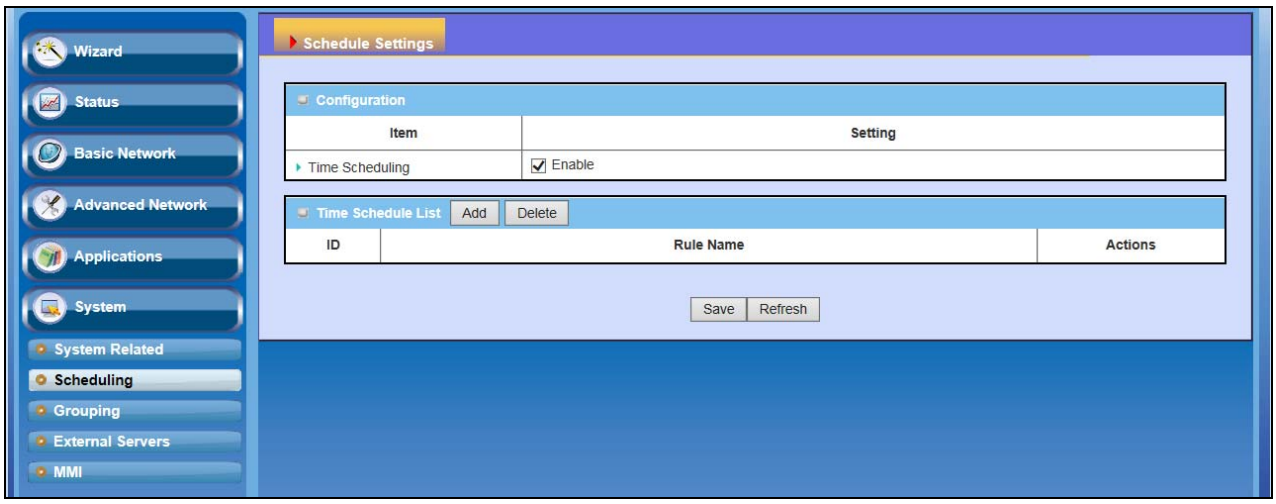


5. **Reboot:** You can also reboot this device by clicking the “Reboot” button.
6. **Reset to Default:** You can also reset this device to factory default settings by clicking the “Reset” button.
7. **Wake on LAN**: Wake on LAN (WOL) is an Ethernet networking standard that allows a computer to be turned on or awakened by a network message. You can specify the MAC address of the computer, in your LAN network, to be remotely turned on by clicking on the “Wake up” command button.
8. **Backup Configuration Settings**: You can backup your settings by clicking the “Backup” button and save it as a bin file. Once you want to restore these settings, please click Firmware Upgrade button and use the bin file you saved.

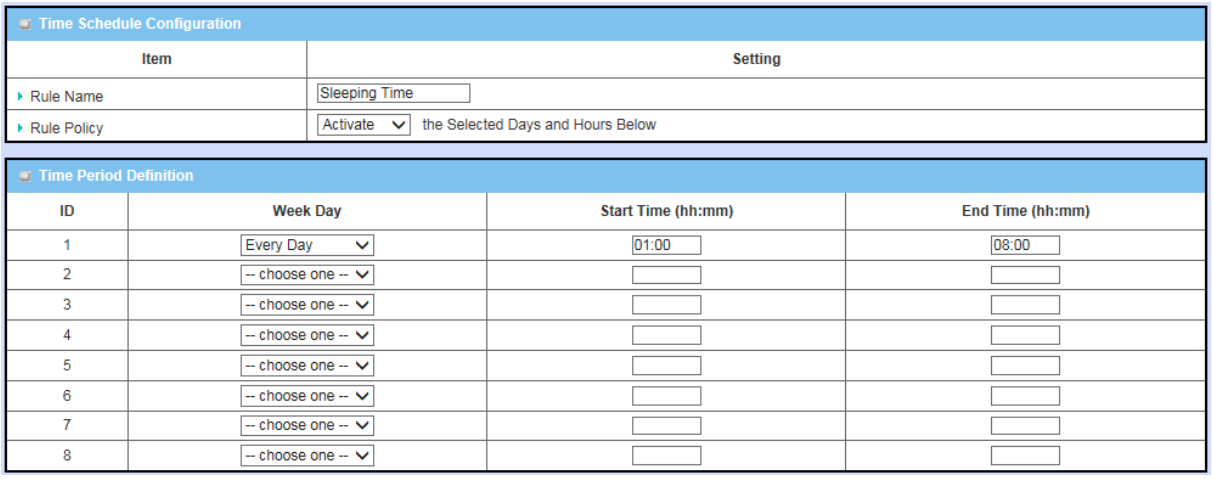
Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.4.2 Scheduling

You can set the schedule time to decide which service will be turned on or off. The added rules will be listed as below and they can be up to 100 rules.



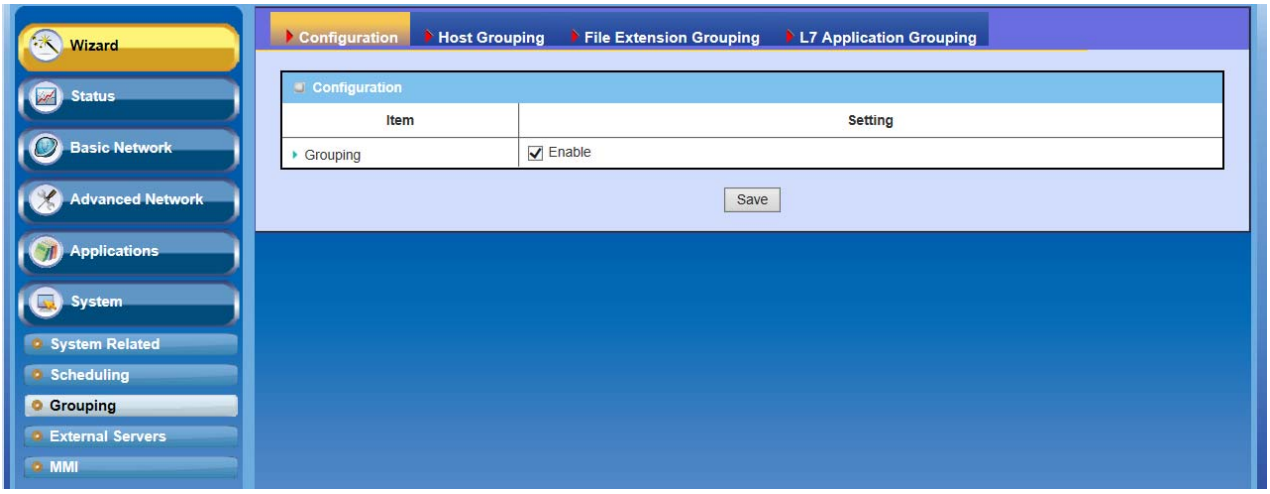
1. **Enable:** Enable or disable the scheduling function.
2. **Add New Rule**: To create a schedule rule, click the “Add New” button or the “Add New Rule” button at the bottom. When the next dialog popped out you can edit the Name of Rule, Policy, and set the schedule time (Week day, Start Time, and End Time). In a schedule rule, it collects 8 time periods to organize it. You also can specify the rule is to define the enable timing (“Inactive except the selected days and hours below”) or disable timing (“Active except the selected days and hours below”).



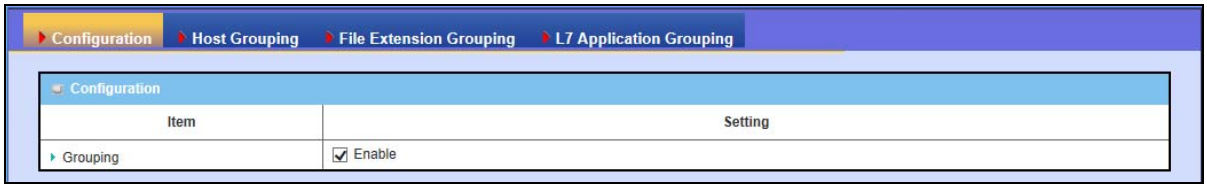
Afterwards, click **“save”** to store your settings or click **“Undo”** to give up the changes.

3.4.3 Grouping

This device supports three types of objects to be grouped. They are host objects, file extension objects and L7 Application objects. One “Enable” checkbox provides user to activate the grouping function for all types of objects.



3.4.3.1 Grouping Configuration



1. **Grouping**: Check the “Enable” box to activate the grouping function.

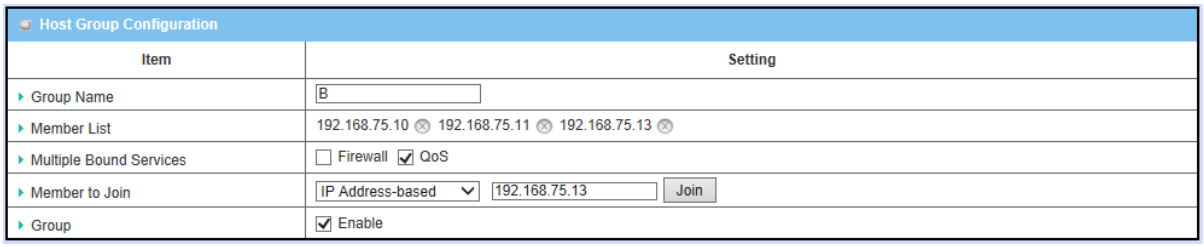
3.4.3.2 Host Grouping

3.4.3.2.1 Host Group List

Host Group List can show the list of all host groups and their member lists and bound services in this window. You can add one new grouping rule by clicking on the “Add” command button. But also you can modify some existed host groups by clicking corresponding “Edit” command buttons at the end of each group record in the Host Group List. Besides, unnecessary groups can be removed by checking the “Select” box for those groups and then clicking on the “Delete” command button at the Host Group List caption.

1. **Add**: Click on the button to add one host group.
2. **Delete:** Click on the button to delete the host groups that are specified in advance by checking on the “Select” box of those groups.
3. **Edit**: Click on the button to edit the host group.
4. **Select:** Select the host group to delete.

3.4.3.2.2 Host Group Configuration

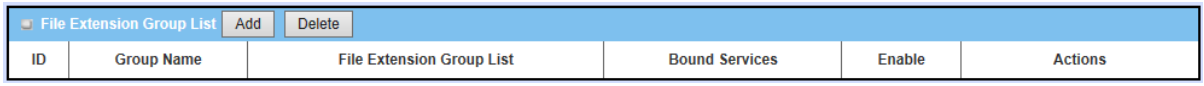


1. **Group Name**: Define the name of group.
2. **Member List:** Show the list of members that have joined the group. A delete button '⊗' is behind each member and can be used to remove the member from the group.
3. **Multiple Bound Services**: The defined group object can be used in various applications, like Firewall or QoS&BWM.
4. **Member to Join:** To define a member by using IP address or MAC address. Choose "IP Address-based" or "MAC Address-based" first and then type specific value for the member. Click on the "Join" button to join the member in the group.
5. **Group:** Check the "Enable" box to activate the group definition.

3.4.3.3 File Extension Grouping

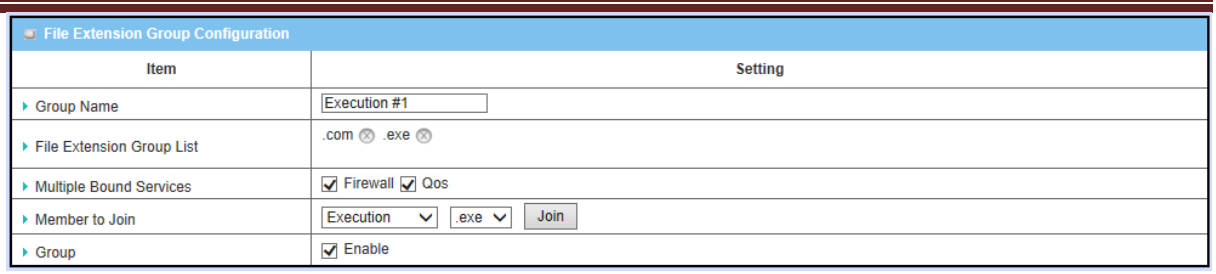
3.4.3.3.1 File Extension Group List

File Extension Group List can show the list of all file extension groups and their member lists and bound services in this window. You can add one new grouping rule by clicking on the "Add" command button. But also you can modify some existed file extension groups by clicking corresponding "Edit" command buttons at the end of each group record in the File Extension Group List. Besides, unnecessary groups can be removed by checking the "Select" box for those groups and then clicking on the "Delete" command button at the File Extension Group List caption.



1. **Add**: Click on the button to add one file extension group.
2. **Delete:** Click on the button to delete the file extension groups that are specified in advance by checking on the "Select" box of those groups.
3. **Edit**: Click on the button to edit the file extension group.
4. **Select:** Select the file extension group to delete.

3.4.3.3.2 File Extension Group Configuration

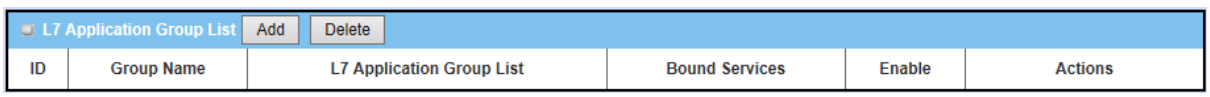


1. **Group Name**: Define the name of group.
2. **Member List:** Show the list of members that have joined the group. A delete button ⊗ is behind each member and can be used to remove the member from the group.
3. **Multiple Bound Services**: The defined group object can be used in various applications, like Firewall or QoS&BWM.
4. **Member to Join:** To define a member by selecting a file extension type category and a file extension name. File extension categories include “Image”, “Video”, “Audio”, “Java”, “Compression” and “Execution”. And each category has its own list of file extension objects, like “.exe”. Choose one to join the group by clicking on the “Join” button.
5. **Group:** Check the “Enable” box to activate the group definition.

3.4.3.4 L7 Application Grouping

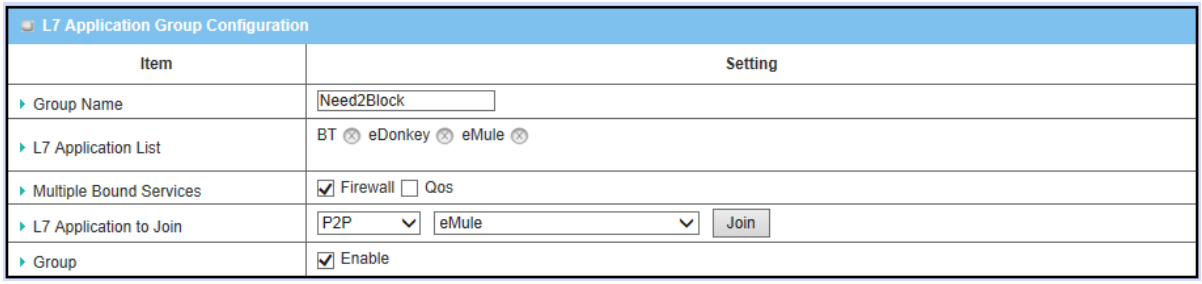
3.4.3.4.1 L7 Application Group List

L7 Application Group List can show the list of all file extension groups and their member lists and bound services in this window. You can add one new grouping rule by clicking on the “Add” command button. But also you can modify some existed file extension groups by clicking corresponding “Edit” command buttons at the end of each group record in the File Extension Group List. Besides, unnecessary groups can be removed by checking the “Select” box for those groups and then clicking on the “Delete” command button at the File Extension Group List caption.



1. **Add**: Click on the button to add one L7 application group.
2. **Delete:** Click on the button to delete the L7 application groups that are specified in advance by checking on the “Select” box of those groups.
3. **Edit**: Click on the button to edit the L7 application group.
4. **Select:** Select the file extension group to delete.

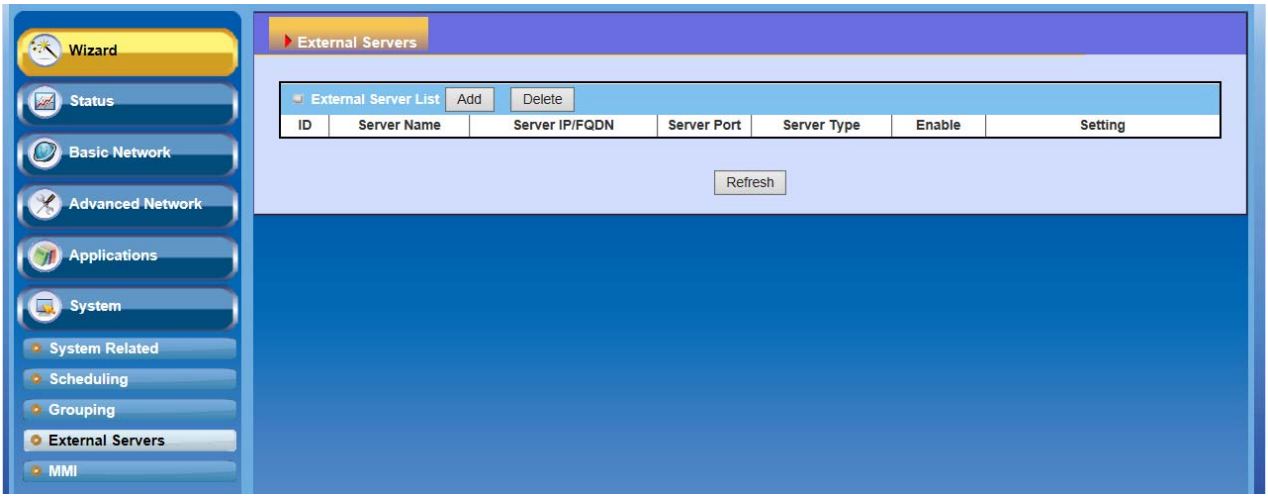
3.4.3.3.2 L7 Application Group Configuration



1. **Group Name**: Define the name of group.
2. **Member List:** Show the list of members that have joined the group. A delete button ⊗ is behind each member and can be used to remove the member from the group.
3. **Multiple Bound Services**: The defined group object can be used in various applications, like Firewall or QoS&BWM.
4. **Member to Join:** To define a member by selecting a L7 application category and an application name. L7 application categories include “Chat”, “P2P”, “Proxy” and “Streaming”. And each category has its own list of L7 application objects, like “eMule”. Choose one to join the group by clicking on the “Join” button.
5. **Group:** Check the “Enable” box to activate the group definition.

3.4.4 External Servers

This device supports six types of external server objects to be created. They are Email Server objects, Syslog Server objects, RADIUS Server objects, Active Directory Server objects, LDAP Server objects and UAM Server objects. These objects can be used in other applications of system, like system log emailing to email server or sending to syslog server in **[System]-[System Related]-[System Status]**, captive portable function in **[Applications]-[Captive Portable]**, SMS forwarding to email server or syslog server in **[Applications]-[Mobile Applications]-[SMS]**, AP Management alerting system in **[Applications]-[AP Management]**, and IO Management alerting handler in **[Applications]-[IO Management]**. Above usage examples depend on the provided functions of different product models.



3.4.4.1 External Server List

External Server List can show the list of all defined external server objects and their attributes in this window. You can add one new external server object by clicking on the “Add” command button. But also you can modify some existed external server objects by clicking corresponding “Edit” command buttons at the end of each object record in the External Server List. Besides, unnecessary objects can be removed by checking the “Select” box for those objects and then clicking on the “Delete” command button at the External Server List caption.

External Server List Add Delete

ID	Server Name	Server IP/FQDN	Server Port	Server Type	Enable	Setting
1	JPEmailAccount	email.amit.com.tw	25	undefined	☑	Edit ☑ Select
2	JPEmailAccount	email.amit.com.tw		Email Server	☑	Edit ☐ Select

1. **Add**: Click on the button to add one external server object.
2. **Delete:** Click on the button to delete the external server objects that are specified in advance by checking on the “Select” box of those objects.
3. **Edit**: Click on the button to edit the external server object.
4. **Select:** Select the external server object to delete.

3.4.4.2 External Server Configuration

External Server Configuration save

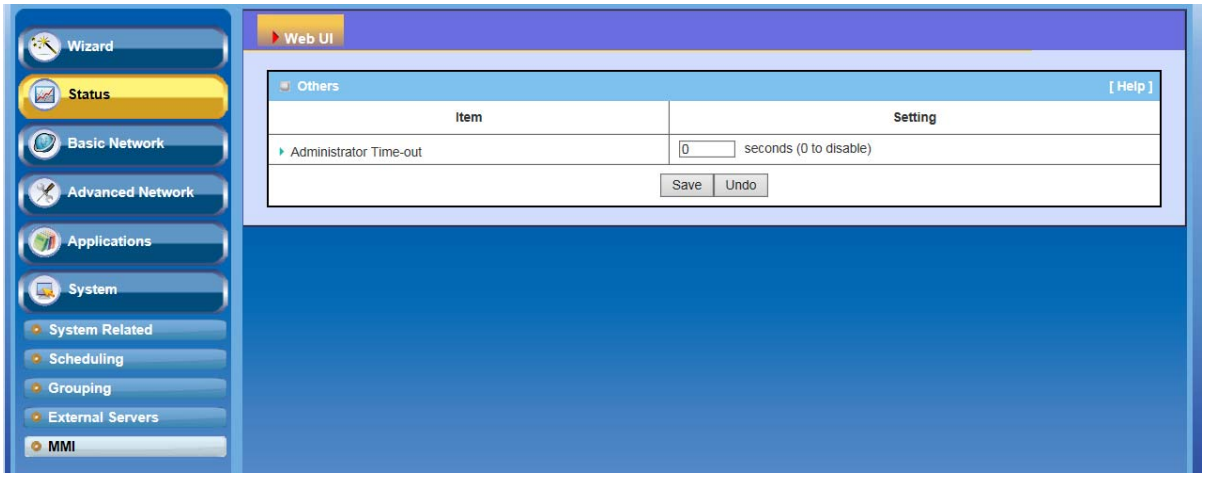
Item	Setting
Server Name	JPEmailAccount
Server IP/FQDN	email.amit.com.tw
Server Port	
Server Type	Email Server User Name: jp Password: ••••••
Server	☑ Enable

1. **Server Name**: Define the name of external server object.

2. **Server IP/FQDN:** Specify the IP address or domain name of external server.
3. **Server Port:** Specify the service port of external server.
4. **Server Type:** Select one server type from the option list of “Email Server”, “Syslog Server”, “RADIUS Server”, “Active Directory Server”, “LDAP Server” and “UAM Server”. Based on your selection, there are several parameters need to specify. When you select “Email Server” option for the Server Type, you must specify two more parameters, “User Name” and “Password”. When “Syslog Server”, no more parameter is required. When “RADIUS Server”, you can specify primary RADIUS server and secondary RADIUS server for redundancy. For each server, following parameters need to be specified: Shared Key, Authentication Protocol (CHAP or PAP), Session Timeout (1~60 Mins) and Idle Timeout (1~15 Mins). When “Active Directory” Server, you must specify one more parameter, “Domain”. When “LDAP” Server, one more parameter, Base Domain Name. When “NT Domains” Server, one more parameter: “Workgroup”. When “UAM” Server, following parameters must be provided: “Login URL”, “Shared Secret”, “NAS/Gateway ID”, “Location ID” and “Location Name”. Among them, Location Name is optional.
5. **Server:** Check the “Enable” box to activate the external server object.

3.4.5 MMI

3.4.5.1 Web UI



You can set UI administration time-out duration in this page. If the value is “0”, means the time-out is unlimited.

Appendix A. Licensing Information

This product includes copyrighted third-party software licensed under the terms of the GNU General Public License. Please refer to the GNU General Public License below to check the detailed terms of this license.

Availability of source code

Please visit our web site or contact us to obtain more information.

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only only if its contents constitute a work based on the Program (independent of having been made by running the

the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software

Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES,
INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS